Kakinada Smart City Corporation Ltd.

RFP NO. KSCCL/ System Integrator/2016/ 1

Request for proposal for Selection of System Integrator for Development & Implementation of Smart *Kakinada* City Solutions

Dt. 19-12-2016

Volume 2: Scope of Work

Managing Director
KSCCL
Kakinada

For further information please contact:
Email id: kakinadacorporation@gmail.com
smartcityofficekkd@gmail.com

Website: www.kakinadacorporation.ap.gov.in

CONTENTS

1.0 Current Status of Implementation of e-Gov. Citizen Centric Applications:

All the e-Gov. services of Kakinada Municipal Corporation are being operated successfully in digital mode for quite some time, in improving the efficiency and greater interaction with citizens.

Sincerity in usage of the online interactive services by KMC, is well reflected in speedy clearance and redressal of public grievances, in reaching a disposal rate of 96%. Digital services are being extensively used by public through various platforms like, Help desks, Mee Sewa& Call Centres and through internet of things. 120 CCTV cameras have been installed and are in use for surveillance in which live videos are being analyzed for follow up and quick, decision support for actions to be taken towards mitigation of various critical scenarios.

Public Grievances Analytics

Sl. No	Type of Grievance	Percentage of Disposal
1	Public Health Services	96.39
2	Street Lights	98.58
3	Water Supply	84.67
4	Town Planning	81.25
5	Urban Poverty Alleviation	100.00
6	Revenue	96.34
7	Administration	100.00

1.1 Current Status of Operations of Command and Control Centre (CCC):

Nine seated Command and Control Centre has been established in Police Control Room and has eight 55" LG TVs for Television displays. The following table describes Bill of Material and brief specifications of current infrastructure:

Sl. No	Item	Make, Model/ Brief Specifications	Quantity
1	TV	55" LG TVs	8
2	Operators	Custom-made office cubicles	9
3	Operator Desktop	Dell OptiPlex 3040 desktops	9
4	UPS	Compaq 6 KVA UPS	2
5	Networking Equipment	Managed switch, LAN & Media Converter	1 Rack

Live feed from 120 field cameras is being accessed and analyzed for further decisions and quick actions of surveillance. The CCC has two 24 port manageable switches with two Dell R 750 Servers operating on Windows 2008 Version R2 platform with milestone tool set being used for media archival and for various data analytics.

1.2 Performance of some of the e-Gov Citizen Centric applications and their public outreach with accrued work efficiency have been elucidated herewith:

S. No.	Service Portfolio	Hosted By	Update Frequency	Other Details	Efficiency in Performance %
1	Street Lights	EESL	On click	Live monitoring of performance of street lights	98.58
2	Solid Waste Management- Bin Monitoring	Existing Vendor	Daily basis	Supervisors take pictures of the bin and upload.	67.33
3	Solid Waste Management – Vehicle Tracking System	Existing Vendor	Tracking on hourly basis	Live status of vehicles is being monitored	91.50
4	Surveillance Cameras at Police Control Room	Existing Vendor	Live feed & Analytics	Feed from 120 Cameras	Operational
5	Citizen Complaints	Existing Vendor	Hourly	Redressal on priority basis	96.00
6	Citizen Requests	Existing Vendor	Hourly	Are being addressed very promptly.	92.00

2.0 Scope of Project Works:

The key components of Smart Kakinada City solutions include:

1. Kakinada City Network
2. Kakinada City Wi Fi Connectivity
3. Kakinada City Surveillance System – Command and Communications Centre
4. ICT Enabled Solid Waste Management
5. Smart Lighting
6. Smart Traffic
7. Smart Parking
8. Solar Power based Environmental Sensors
9. Smart Governance and Citizen Services
10. Health Information System
11. Human Resources Management System – Teachers, Schools, School Buildings, Schemes Monitoring – Mid Day Meal Scheme, Sarva Shiksha Abhiyan, Teacher and Student performance monitoring systems, etc.
12. Office Management System – File Tracking System, Personnel Information System, Budget and Expenditure Monitoring System inclusive of tracking of tax payments, Leave Monitoring System, Biometric Attendance, setting up of Video Conferencing System, Key Performance Indicators based Employee Performance Monitoring System, etc. – on Intranet portal
13. Water Resources Management System
14. Asset Inventory Management System
15. Welfare Schemes Management
16. Web & Intranet Portals
17. Data Centre, Disaster Recovery Centre (Cloud based), ICT Infrastructure Development
18. Smart devices, Sensors & Infrastructure Installations, Operations and Maintenance
19. Setting up of Network Connectivity and Provision of Technical and Operational Support
20. Training and Handholding Sessions, etc.

The above components shall be developed, supported and operated in close coordination between the following entities:

1. Command Control Centre (CCC)
2. Kakinada Operations Centre
3. Data Centre and Disaster Recovery Centre (DC & DRC)
4. Administrative controlled Intranet portal of the Authority
5. Central Apex Core Committee for provision of technical consultancy, to review plans, procedures, target based achievements, quality of works and to provide timely advisories for smooth and efficient operations
6. Selected System Integrator’s (SI) teams would be undertaking Pre-Implementation phase, Implementation Phase and Post Implementation phase of the above listed activities.SI would also consider integration and syncing of activities taken up by existing vendors for their smooth continuity of operations.

The bidders shall be responsible to carry out the detailed survey prior to submission of bid for the complete solution to capture component-wise requirements in order to finalize infrastructure, network bandwidth, operational & administrative requirements and challenges thereon. Subsequent sections deal with the solution, scope, requirements, etc. The SI shall note that the activities defined within scope of work mentioned in the document, are indicative only and may not be exhaustive. SI is expected to perform independent analysis for carrying out any additional works, to fulfil the requirements as mentioned in the RFP and factor all of them in its response.

2.1 Project Implementation Timelines, Deliverables and Payment Terms:

Authority intends to implement the project in a phased manner, distributed in two phases as mentioned below. **However, to handle the priorities and development & implementation of prominent applications on priority basis, which include setting up of Central Command Centre and integrating sensitive citizen centric e-Gov. applications for capturing critical data on citizens' welfare & development on day to day basis and address detailed analytics for quick decision support and policy making to improve overall efficiency of functioning of all departments under KMC. These applications will be detailed during the initial survey period in close consultation with various stakeholders.**

2.2. Project Deliverables, Milestones and Timelines:

S. No.	Milestone	Deliverables	Timelines (in Months)
A.	**Phase 1**		
1.	**Project Initiation**	Detailed Project Survey Report including infrastructure assessment, phase wise location distribution, hardware deployment plans etc. Detailed Project Plan including Operations management, Contract management, Risk management, Information Security and Business Continuity are required to be worked out.	**T + 1 month**
2.	**Smart Traffic, Parking, Solid Waste, smart governance applications**		**T+3 months**
	Supply, installation, commissioning, training & operationalization of above Smart listed Solutions indicated at item 2.	Delivery Report, inspection reports for each of the components • Site Completion/readiness Report • Software Licenses • Training Completion Certificate • Acceptance /Go Live Certificate from Authority/authorized entity	
3	**Kakinada City Wi Fi connectivity**		**T+3 months**
	Supply, installation, commissioning, training & operationalization of Kakinada Wi Fi at 50% of total identified locations	Delivery Report, inspection reports (component-wise), Site Completion/ readiness Report, Acceptance Certificate from Authority/authorized entity	
4	**Kakinada City Surveillance System**		**T+ 3 months**
	Supply, installation, commissioning, training & operationalization of Kakinada Surveillance at 50% of total identified locations for deployment, installation, commissioning, training and operationalization of zonal layer for Kakinada City network backbone	Delivery Report, inspection reports (component-wise) Site Completion/ readiness Report Software Licenses Acceptance Certificate from Authority/authorized entity (component-wise) Site Completion/readiness Report Software Licenses Acceptance Certificate from Authority/authorized entity	
5	***Kakinada City Network Backbone***		**T+3 Months**
	Kakinada City Network Backbone –Deployment, installation, commissioning,	Delivery Report, inspection (component - wise) Site Completion/readiness Report, Software Licenses Acceptance	

S. No.	Milestone	Deliverables	Timelines (in Months)
	training and operationalization of zonal layer for Kakinada network backbone for 50% of the total identified locations.	Certificate from Authority/authorized entity	
6	**Command Control Center & Kakinada City Operations Center**		**T+3 months**
	Design, supply, installation, commissioning including interior civil work & operationalization of Command Control Center and Kakinada Operation Center including data center and DR set up, Network Operations Center and Helpdesks & Development, Integration and Operation of all e-Gov. Applications	Delivery Report, inspection reports (component - wise) Site Completion/ readiness Report Licenses Acceptance Certificate from Authority/authorized entity	
	Phase 2		
1	**Kakinada City Wi Fi**		T + 9 Months
	Supply, installation, commissioning, training, operationalization & Go Live of Kakinada City Wi Fi at remaining 50% of total identified locations	Delivery Report, inspection reports (component - wise) Site Completion/ readiness Report ·Licenses Training Completion Certificate · Acceptance /Go Live Certificate from Authority/ authorized entity	
2	**Kakinada City Network Backbone**,		T+9 Months
	Deployment, installation, commissioning, training and operationalization of zonal layer for Kakinada network backbone at the remaining 50% of the total identified locations.	Delivery Report, inspection (component - wise) Site Completion/ readiness Report Software Licenses, Acceptance Certificate from Authority/authorized entity	
3	**Kakinada City Surveillance System**		T + 9 months
	Kakinada City Surveillance System - Supply, installation, commissioning, training, operationalization & Go Live of Kakinada City Surveillance System at additional 50% of total identified locations	Delivery Report, inspection reports (component - wise) Site Completion/ readiness Report Software Licenses · Acceptance /Go Live Certificate from Authority/authorized entity	
4	**Operations and Maintenance phase**		T1+60 months
	Operation & Maintenance	SLA Compliance Reports	Every Quarter

Note:

- ***T is the date of signing of contract***
- ***T1 is the date of Go Live of the last Phase=T+9 Months***

2.3. Payment Terms

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

2.4 Payment Schedule

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

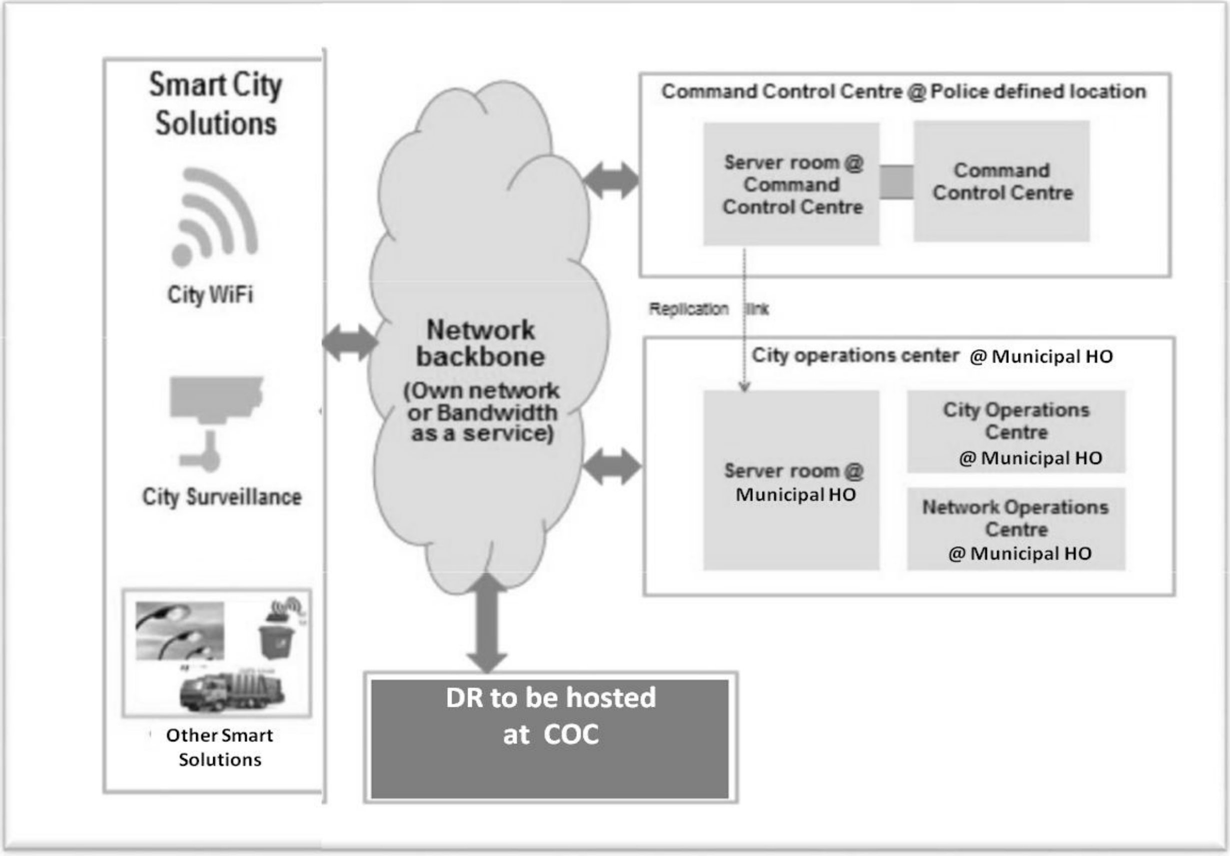
S. No.	Scope of Work	Timelines	Payment
1	Phase I Operationalization & Go Live	T + 3 Months	25% of contract value
2	Phase II Operationalization & Go Live	T + 9 Months	25% of contract value
3.	Operations & Maintenance phase for a period of 60 months from the date of Go Live of the last solution	T1 + 60 Months	50% of Contract Value in equal quarterly installments

Note:

T is the date of signing of contract

T1 is the date of Go Live of the last phase=T+9 Months

3.0 Roles & Responsibilities of System Integrator


Smart City Solutions
City WiFi
City Surveillance
Other Smart Solutions
Network backbone
(Own network or Bandwidth as a service)
Command Control Centre @ Police defined location
Server room @ Command Control Centre
Command Control Centre
Replication link
City operations center @ Municipal HO
Server room @ Municipal HO
City Operations Centre @ Municipal HO
Network Operations Centre @ Municipal HO
DR to be hosted at COC

Diagrammatic representation of scope of work for System Integrator

More specifically, the following indicative activities are to be carried out by the selected System Integrator (SI):

1. Project Planning, execution and Management
2. Assessment and Gap analysis of requirements for all Smart Kakinada city components under scope.
3. Solution Design, System Customization and development for all components.
4. ICT items Procurement, deployment, commissioning and maintenance during the contract period.
5. Site Preparation including required civil works, LAN Networking, Wi Fi connectivity, etc.
6. Conduct of Software Applications and general awareness Training sessions.
7. Business Process Reengineering for the software applications/ services.
8. STQC Certification for third party audit of the developed software applications and ICT solutions.
9. User Acceptance Testing & Go live.
10. Capacity Building
11. Technical, Maintenance and Operational Supports for the developed applications at site for five Years after integrated system go live date.

3.1 Finalization of the Detailed Technical Architecture for Smart Kakinada City Network:

The SI 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 digital video streams to the Command Centers and observation centers for their catalogued archival for analysis, decision support and for the generation of SMS based alerts to officials concerned and citizens at large.

Broad components of the Technical Architecture should comply with:

(a) the published e-Governance latest standards, frameworks, policies and guidelines provided in http://egovstandards.gov.in; and

(b) leading industry standards and/or as per standards mentioned at Annexure –XI.

SI shall submit the detailed Technical Architecture and description of each of the components/ sub-components, along with the technical bid, which should cover the following guiding principles:

- **Scalability** - All technical components of the architecture must support scalability to provide continuous growth to meet the growing demands of the Smart Kakinada city requirements. The system should also support vertical and horizontal scalabilities so that depending on changing requirements from time to time, the system can be scaled upwards. There must not be any system imposed restrictions on the upward scalability in provisioning of number of cameras, data canter equipment or other smart Kakinada city solution components. Main technology components requiring scalability are storage, bandwidth, computing devices and other ICT Infrastructure.

  The architecture should be scalable (cater to increasing load of internal and external users and their transactions) and capable of delivering highest performance. In this context, it is required that the application and deployment architecture should provide for Scale-Up and Scale out on the software applications and Web Servers, Database Servers and all other solution components. The data center infrastructure shall be capable of serving at least 1000 concurrent users. **Optimum usage hybrid model of storage space of local data centre set up along with cloud infrastructure solution inclusive of DRC could also be considered in pay as use mode for provisioning of cost effective and foolproof solutions.**
- **Availability** - The architectural components should be redundant to 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 situations, the systems need to be configured to mask and recover with minimum outage. The SI shall make the provision for high availability of all the services of the system. Redundancy has to be considered at the core/data canter components' level.
- **Security** - The architecture must adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, data theft and from natural disasters, etc. SI 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 data theft should be controlled and well supported (and implemented) with the strong security policies. The virus and worm attacks should be well defended with gateway level with latest versions of Anti-virus system, along with workstation level continuously upgraded strong Anti-virus mechanism. There should also be an endeavour to make use of the SSL/VPN technologies to have secured communications between software applications and its end users. Furthermore, all the system logs should be properly stored & archived for future analysis and forensics whenever required. SI would carry out the security audit of the entire system before handover and after UAT. SI Should also carry out security audit of the implemented systems as and when changes are made and at regular intervals during O&M period.

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

The systems implemented for project should be highly secure, considering that it is intended to handle highly sensitive data relating to the KMC/AP Gov. and also citizens of Kakinada. The security considerations to be adopted in this regard include:

i. Identification, Authentication, Access Controls, Administration and Audit and technical support as per industry standard protocols.

ii. The solution shall support advanced user authentication mechanisms including digital certifications and biometric authentications as deemed necessary.

iii. Security design should provide well-designed identity management system, security of physical and digital assets, data and network security, backup and recovery along with disaster recovery mechanisms.

iv. The solution should make provision for maintaining audit trails of all the transactions and should also ensure the non-repudiation of audit trail without impacting the overall performance of the system.

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

vi. The application design and development should comply with top 10 principles of Open Web Application Security Project (OWASP).

- **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 with the growth of the environment. Network should be auto/manually configurable for various future requirements for the ease of maintenance and debugging.
- **Interoperability** - The system should have capability to access digital feed from field cameras installed by private parties and Govt. agencies at public places, and compress and archive with appropriate cataloguing for analytics, decision support and for much needed real time SMS alerts.
- **Open Standards** - Systems should use open standards and protocols for effective integration with other open source solutions.
- **Single-Sign On-** The application should enable single-sign-on so that any user once authenticated and authorized by system is not required to be re-authorized for completing any of the services in the same session, if the session is not idling for long time or session has not broken down due to network/power failure or other related issues. For employees of the departments concerned, the browser based software application should be accessible on the intranet, through single-sign-on with appropriate authentication mechanism, to provide access to all the services of the departments/sections concerned based on their specific roles and responsibilities. Appropriate online basic and advanced help modules/help desk, for smooth usage of the respective software applications are to be provisioned. Similarly, for citizens and other interested beneficiaries, based on their individual profiles captured through appropriate registration process, the system shall enable single-sign on facility for online submission of applications for various services, make online payments, take reports and look for answers to their queries, lodge complaints and check status of their applications and complaints through online access or receive SMS or alerts as the case may be.
- **Supporting PKI based Authentication and Authorization mechanisms:** The solution shall support PKI based Authentication and Authorization mechanisms, in accordance with IT Act 2000, using the Digital Certifications issued by the Certifying Authority (CA). In particular, three types of authentications, viz., login id & password, biometric and digital signature are required to be implemented by SI for officials/employees involved in the operation of e-Gov. solutions and other sensitive and secured operations.
- **Interoperability Standards-** Keeping in view the evolving needs of interoperability, especially the solution shall become the focal point of delivery of citizen centric services, and may also involve linking of cross-functionalities across various e-Governance projects

of different departments/business processes, etc., the solution should be built on Open Standards. The SI shall ensure that the application developed can be easily integrated with the various applications operational across the country. Accordingly, the code shall not be dependent on any proprietary software, particularly, through the use of proprietary 'stored procedures' belonging to a specific database product, etc.. The standards should comply with:

a) with the published latest e-Governance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in; and

b) leading industry standards and/or as per standards mentioned at Annexure –XI.

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

- Passive networking & civil work during implementation and O&M period,
- Supporting manpower at Command and observation canters & Mobile Vans during post-implementation phase in the contract period.
- FMS staff for non-IT support during post-implementation phase.

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

- **GIS Integration-** SI shall undertake detail assessment for integration of the Smart e-Governance systems, Surveillance System and all other components of the Geographical Information System (GIS). SI is required to carry out seamless integration to ensure ease of use of GIS in the Dashboards in Command Control Centers. If this requires specific field survey, it needs to be done by SI. If such a data is already available with the authority, it shall facilitate to provide the same on demand in advance. SI is required 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.
- **SMS Gateway Integration-** SI shall carry out SMS Integration with the Smart Kakinada City Solution System and develop all needed applications to send mass/individual SMSs to groups/individuals. Any external/third party SMS gateway is being proposed for usage, the same needed to be specified in the Technical Bid, and get the same approved during Bid evaluation process.
- **Application Architecture:**

I. The applications designed and developed for the authority comprising of various Departments and sections concerned, must adopt best practices and industry standards. In order to achieve the high level of stability and robustness of the applications being developed, the Software Development Life Cycle (SDLC) must be adopted and also adopt the requisite security standards and constraints for access and control rights. Various modules of applications should have a common exception manager to handle any kind of exception arising due to internal/external factors. The standards should (a) at least comply with the published e-Governance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and (b) be of leading industry standards and /or as per standards mentioned at Annexure –XI as already envisaged.

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

SI shall design and develop the Smart Kakinada City System as per the Functional and System requirement specifications finalized and as approved by the authority.

I. The Modules specified will be developed afresh based on approved requirements.

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

III. The user of citizen centric services should be given a choice to interact with the system in the local language in addition to English. The application should have provision for uniform user experience across the multi-lingual functionalities covering following aspects:
- Front end web portal in English and also in local language.
- e-forms (Labels & Data entry in local languages). Data entry should be provided preferably using the Enhanced Inscript standard (based on Unicode version 6.0 or later) keyboard layout with option for provision of floating keyboard.
- Storage of entered data in local language using UNICODE (version 6.0 or later) encoding standard.
- Retrieval & display in local language across all user interfaces, forms and reports with all browsers compliant with Unicode version 6.0 and above.
- Facility for bilingual printing (English and Telugu)

IV. Application should have a generic workflow engine for citizen centric services. This generic workflow engine will allow easy creation of workflow for new services. At the minimum, the workflow engine should have the following features:
- Feature to use the master data for the auto-populating the forms and dropdowns
- Creation of application form, by "drag & drop" features using meta data standards
  i. Defining the workflow for the approval of the form
  ii. Submitted applications of Citizens to be considered for processing in First in First out or as per priorities assigned.
  iii. Defining citizen charter/delivery of service in a time bound manner
- Generation of the "output" of the service, i.e. Certificate, approval Order, etc., Automatic reports of compliance to citizen charter on delivery of services and delay reports

Standards adopted should comply with:

a) with the published latest e-Governance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in; and

b) leading industry standards and/or as per standards mentioned at Annexure –XI.

V. The application should have a module for management of digital signature including issuance, renewal and suspension of digital signatures based on the administrative decisions taken by the State.
- SI shall ensure usage Digital signatures/e-Authentication (Aaadhaar Based) to authenticate approvals for service requests etc.

VI. e-Transaction & SLA Monitoring Tools

A. The SI should be able to measure and monitor the performance of the deployed infrastructure and all SLAs set out in this RFP. More importantly, it should be possible to monitor in REALTIME, the number of citizens accessing e-Services in a day, month or year, through appropriate tools and MIS reports.

B. The Infrastructure management and Monitoring System shall be used by SI to monitor the infrastructure (Both IT and Non-IT) hosted at the Data center and DR site.

C. For monitoring of uptime and performance of IT and non-IT infrastructure deployed, the SI shall have to provision for monitoring and measurement tools, licenses, etc. required for this purpose.

VII. The Smart Kakinada City solution should have roadmap to integrate with key e-Gov initiatives of the State, namely, Portal Services, Citizen help desks, Certifying Authority, etc.

VIII. Mobile enablement of all the Smart Kakinada City e-Gov. solutions.

3.2 Other expectations from SI:

1. SI shall engage in active consultations at the earliest with the Authority, Kakinada Police Administration and other key stakeholders to establish a clear and comprehensive project plan in line with the priorities of all project stakeholders and the project objectives.
2. Study the existing fiber duct (if any) layout in the city and existing network to understand the adopted technologies in each of the following areas but not limited to:
   I. Kakinada City Wide Wi Fi Connectivity
   II. Surveillance Infrastructure – CCTV Camera set up, Data communication mechanisms, control room and Infrastructure
   III. Other Smart Kakinada City e-Gov. initiatives already envisaged
3. SI shall assess existing capacity and potential of ICT infrastructure to support the entire solution in use and integrate the same with the proposed solution as per applicability.
4. SI shall judiciously evaluate the resources and duration planned for undertaking the current state assessment, given the overall timelines and milestones of the project.
5. SI shall be responsible for supply of all the Products/equipment such as optical fiber cable, Network, Hardware, Software, Devices, etc. as indicated (but not limited to) in the tentative Bill of Materials included in the RFP and their appropriate quantity & capacity for the envisaged Smart Kakinada City Solutions.
6. SI shall be responsible for supply of passive components indicated in the Bill of Materials section of the RFP viz. Housings, Fiber Patch Cords, Racks etc. Civil works required for the site shall also be undertaken by the SI.
7. Validate & Assess the reuse of the existing ICT infrastructure, if any, already with Authority.
8. Supply, Installation, Commissioning and maintenance of entire solution at all the locations.
9. SI shall provide the bandwidth required for operationalizing each Smart Kakinada City initiative till the time Authority's own fiber is made ready by the SI as part of the scope of work of this RFP. The bandwidth requirement shall be analyzed and procured by the SI at its own cost/risk.
10. SI shall Install and commission connectivity across all designated locations.
11. SI shall establish high availability, reliability and redundancy of the network elements to meet the Service Level requirements.
12. SI shall be responsible for planning and design of the access network architecture (access controllers, backhaul connectivity, routers, switches, etc.) to meet the ICT infrastructural and service requirements for all smart Kakinada city ICT initiatives.
13. SI shall be responsible for upgradation, enhancement and provisioning additional supplies of network (including active/passive components), hardware, software, etc. as per the requirements of the Authority.

14. SI shall ensure that the infrastructure provided under the project should have validity for atleast two to three years' life time from the date of bidding.
15. SI shall ensure that the uninterrupted maintenance support and assistance is provisioned during the contract period and five years thereafter.
16. SI shall ensure compliance to all mandatory government regulations as amended from time to time.
17. The SI shall ensure that all the peripherals, accessories, sub-components required for the satisfactory implementation of all the functionalities and complete implementation and operation of the solution being provisioned, including but not limited to devices, equipment, accessories, patch cords (fiber), cables, software, licenses, tools, etc.
18. Authority shall not be responsible if the SI has missed out some components, sub-components, assemblies, sub-assemblies as part of Bill of Materials in the RFP. The SI shall have to provision these & other similar things to meet the solution requirements at no additional cost and time implications to the Authority.
19. All the software licenses that the SI proposes shall be perpetual along with maintenance, upgrades and updates for the duration of the contract. The software licenses shall not be restricted based on location and Authority shall have the flexibility to use the software licenses for other requirements, elsewhere, as per requirements.
20. The SI shall ensure there is a 24x7 comprehensive onsite support for the duration of the contract for all the components and services as per SLA. The SI shall ensure that all the OEMs have an understanding of the service levels required by Authority. SI is required to provide the necessary MAF (Manufacturer Authorization Form) as per the format provided in the RFP in support of OEMs for active support in the project.
21. Considering the criticality of the infrastructure, SI is expected to design the solution considering the RFP requirement of no single point of failure with high level of redundancy and resilience to meet the network uptime requirements.
22. SI shall be responsible for periodic updates & upgrades of all equipment, cabling and connectivity provided at all locations during the contract period.
23. SI shall be responsible for setting up/building/renovating the necessary physical infrastructure including provisioning for network, power, rack, etc. at all the locations.
24. SI is expected to provide following services, including but not limited to:
    i. Provisioning hardware and network components of the solution, in line with the authority's requirements as assessed and approved.
    ii. Size and provision for network devices (like Router, switches, security equipment including firewalls, IPS/IDS routers, etc.) as per the location requirements with the required components/modules, considering redundancy and load balancing in line with RFP.
    iii. Size and provision the WAN bandwidth requirements across all locations considering the application performance, data transfer, DR and other requirements for the Smart Kakinada City ICT initiatives.
    iv. Size and provision the internet connectivity for Service Provider network and Network Backbone.
    v. Size and provision for bandwidth as a service for operations of Kakinada City wide Wi Fi, Kakinada City Kiosks, CCTV surveillance till operationalization of network backbone
    vi. Liaise with service providers for commissioning and maintenance of the links.
    vii. Furnish a schedule of delivery of all IT/Non-IT Infrastructure inventory
    viii. All network equipment proposed as part of this RFP shall be rack mountable.
    ix. Authority may at its sole discretion evaluate the hardware sizing document proposed by the SI. SI needs to provide satisfactory explanation on sizing requirements to the Authority

x. Complete hardware sizing as per the scope of authority approved requirements with provision for upgrade

xi. Specifying the number and configuration of the racks (size, power, etc.) required at all the locations.

xii. The SI shall provide for all required features like support for multiple routing protocols, congestion management mechanisms and Quality of Service support.

xiii. The SI shall ensure that all active equipment (components) are Simple Network Management Protocol (SNMP) V3 compliant and are available for maintenance/ management through SNMP from the date of installation by a Network Monitoring System.

4.0 Enterprise Resource Planning (ERP)

4.1 Salient Features

Various features envisaged for the proposed ERP system in Authority, which are also briefly elucidated the Scope of project works at 2.0 above, are being elaborated here:

a. <u>Architecture</u>

- 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.

b. **User Interfaces**

- 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. o Disparate information can be consolidated from a number of systems as required to produce reports and carry out ad hoc analysis and reporting

c. **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

d. **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)

e. **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. Mee Sewa Centres & Call Centres
    iii. Mobile Apps

f. **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 & e-Governance Core Application. Various indicative integration points are mentioned in the subsequent sections.

g. **Mobile Apps**

- 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 Wireless Access Protocol (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 mechanisms to get and receive information using SMS service.

h. **Web & Intranet Portals**

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 Kakinada City (such as history, heritage details, city guide), Details of Kakinada Municipal Corporation (Elected Political Members, Mayor, Municipal Commissioner of the city, Budget, Administrative Wing, Zonal Information, etc.) various Citizen Centric details/applications, grievance Redressal mechanism, 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), Mee Sewa Centres, Call Centres, Help Desks, (MSC), 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. Citizen will be able to fill the form electronically (both online and offline) through internet services including MSC outlets and submit his/her application electronically. 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 MSC/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 four or more design templates for the new Web portal for Authority from which one of the design template would be selected by Authority.

i. **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.

j. **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.

4.2 Roles of Users in ERP

Sl. No.	Roles	Users
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- Profile login password & 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- a. No activity is performed by user after login for a specified time e.g. 10 minutes. b. User accidentally closes the portal window during login session.	SI/System Admin
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

4.3 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 Gender 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.

Sr. No	Functional Requirement Specifications - Web Portal- User Management
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.
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.

For the design and development of **intranet portal** for the Authority for having exclusive access to employees of the Authority, same rules of user creation and authentication may be followed in addition to provisioning of device MAC no. being used by the official and also the domain in which the user is accessing the system. Messages and alerts would also be required to be provided on mobile and other user interfaces. It will also have system administration module for creation of user ids for various roles and responsibilities as per the official levels of officials for access to various privileges. Important applications in the intranet portal would be

- ✓ Employees Information System having unique Employee ID
- ✓ Payroll Package
- ✓ Leave Monitoring System
- ✓ Biometric based Attendance System
- ✓ Employee Performance Monitoring System, etc.

A. Profile Management:

- Enable registered users to manage their accounts and profiles and as appropriate

B. **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:

I. General Requirements

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

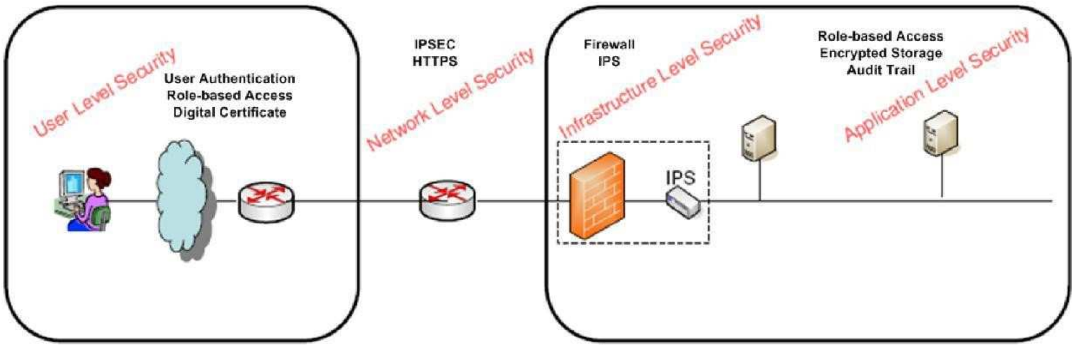
ii. The security measures adopted should be of wide range and of high quality, to create confidence in the systems security and integrity. The system should be protected against deliberate or accidental misuse that might cause a loss of confidence in it or loss or inconvenience to one or more of its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

II. Security Requirements for Portal

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

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 with special characters),

d. Alphanumeric password standards,

e. Minimum number of numeric characters,

f. Non-dictionary words,

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 minimum functionalities:

   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 MSC/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 are 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.

4.4 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.

A. Specifications:

#	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.

#	Item	Minimum Specifications
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
4.	Resolution	• 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

4.5 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

x. Security techniques and measures provide security measures to protect information belonging to the Portal and the entities (departments) from unauthorized access, modification, or deletion.

xi. Monitor, log and audit security incidents with date/time stamping.

xii. Maintain and ensure data integrity and visitors' confidentiality and privacy.

xiii. 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.

xiv. 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.

xv. 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

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

4.6 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.

4.7 Workflow Management System:

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.

A. 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).

B. **General**

- ❖ The system requires continuous availability on 24 X 7 basis.
- ❖ 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 / Wi Fi/ Internet

4.8 Mee Sewa & Call Centres' (MSC) Module:

Roles	Users
A] Citizen Help Desk	
Facility to lodge New Complaints, Check Status	MSC
Facility to check citizen data, Bill Dues, Application Status, Payment Status, Renewal Status, Certificates issuance	Inter & Intranet
Citizen Charter	MSC, Authority
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)	Authority
Fees to be accepted	Accounts
Generate Token of Application acceptance	
Rejection Note in case of inadequate application	
Delivery of the output through CCC / Internet / KIOSK	Intranet

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.,	
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	
Enrolment and Registry Enrolment of firms. (PEC & PRC)	Property Tax, GIS
Details of firms along with their contact details, address, etc.	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,	
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 / KIOSK, Department-wise	
Officer-wise list of services pending	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

4.9 Document & Workflow Management System

Roles	Users
A] File Tracking System	
Scanning & Marking the inward to the respective department	MSC
▪ Incorporation of separate hierarchy for RTI letter movements & Commissioner Office. ▪ Fresh applications ▪ Appeals	MSC, Web, KIOSK
Tracking of the Inward	MSC
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	Authority

4.10 Property Tax Department

Roles	Users
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	Internet, GIS
Option to the citizens to submit their Assessment for confirmation	GIS, Auth.

D] System based calculation of Rateable 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, 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	
Objection, Hearing	
Property Billing, Individual flat-wise billing, Property wise billing, Calculation of Property Tax as per prevailing Stamp Duty for different areas.	Accounts
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 Dishonour 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
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
J] Other Requirements	
Data Porting / Data Entry Suite	
Query of Property Dues	MSC, Web Portal
Scope to link up to Land Records / Registration system	

4.11 License Module (Shops / Food / Market)

Roles	Users
A] Citizen Services	
Issue of New License (Food, Market, Hawkers, Gumasta, etc.)	MSC, 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, License Holder's Details – One or multiple owners, Capture of Mobile No./ E-Mail ID, License holder's photograph(s) (optional), Link to Property Number (optional), License Details – Temporary/ Permanent License, Name of Business, Business Address, Business Details; Trade/ Business Details – License Type, Subtype - multiple levels to define types and sub types. License type, sub-type, unit of measure wise license amount.	GIS, Property Tax Assessment, Professional Tax sub-module
Calculation of License Fee, License Certificate	Accounts
C] Other Departmental Process	
Scrutiny of Applications	Internet

Roles	Users
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
E] Other Requirements	
Data Porting / Data Entry Suite	

4.12 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	

Functionality	Integration required with
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
Fire Safety NOC	
B] Defining Charges	
Development Charges	Accounts
Scrutiny Charges	Accounts
Other Charges	Accounts
C] Departmental Process	
Scrutiny of Applications	GIS, HRMS, Internet
Alerts to inter departmental Officers as per timelines of approving or rejecting proposals	
Site Reports	
NOCs from different departments	Internet
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	Internet
Building Permissions / Occupancy Certificates taken for a particular period	GIS
List of Building Permissions taken but Occupancy Certificate not Taken	

Functionality	Integration required with
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	Web, Projects, SWM, Water
G] Additional Requirements	
Generate Drill Down Progress Reports	Web
Hearing of Grievance Case registered in respect to the Building permission/Building Utilization, etc.	

4.13 Water Connection Module

Roles	Users
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, Consumer Details- Property Details, Owners Details, Link to Property No., Metered/ Non Metered Connections, Multiple Usage type – Domestic, Commercial, etc., Tariff Category.	Property Tax, GIS

Roles	Users
Connection Details- 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, Meter Reading Data Entry, Meter Cut off-Restoration	
Uploading of captured site scrutiny data into the system at department	
Temporary Disconnection	SMS
Bill Generation, Billing for Metered and non-metered connections, Billing schedule for different connection category, Consideration of advance paid if any, Interest calculation on arrears, Bill correction	Accounts, SMS
Bill Printing	
Collection from CCC	Accounts
Handling Cheque dishonour 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	

Roles	Users
E] Other Requirements	
Data Porting / Data Entry Suite	
Query Water Dues	MSC, Internet
Scope for integration with SCADA system (Meter Reading)	

4.14 Accounts & Audit Modules

Roles	Users
A] Masters	
Account Head Definition	
Account Grouping and Sub-Grouping	
Bank Account Details	HRMS
Vendor Details	Procurement System
B] Departmental Process	
Budget Preparation, Distribution and Management System, Budget Classification, Department-wise estimated provision, revision for income and expenditure, Budget Appropriation between different budget heads through approval process, Administrative approval/ disapproval of works linked to budget availability	Procurement, Materials Management, Central Stores, CMSO, other related departments
Receipts through Internet / MSCs / KIOSKs, Counter-wise Collection Detailed and Summary Reports, Revenue Stamp Management, Cheque/ Cash Deposit Slips into Bank, Capture of Cheque Dishonour cases, Remittance entry	All Departmental modules
Payment Management	All Departmental modules
➢ Bill / Liability Entry ➢ Payment Authorization ➢ Payment Voucher (Full or Partial Amount) ➢ Maintaining Check details, Check Printing ➢ Recording of Check Issuance Details ➢ Recording of Cheque Cancellation details ➢ Types of Discounts (Recommending Authority for discounts) ➢ 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 ✓ Maintenance of Loan Details ✓ Alerts for Loan Instalment Payments ✓ Loan Instalment Payments ✓ Generate Bill and Carry out payment ✓ Interest Calculation	
Grants Management - Maintenance of Grant Details,	

Roles	Users
Timing of Grant (Regular/Irregular), Utilization Details, Interest Calculation, Utilization Certificates, Generate alerts for Grant Received or not.	
Debt Management	
Accrued Payment Management / Fund Management	
Investment Management, Maintenance of Investment Register, Alerts on due dates, Comparison of different options for Investments, Interest Calculation, FD Register, 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	Intranet
Outstanding Bill Register	
Reports on Receivables	
Reports on Payables	
Cash Book (Detailed & Summary)	
Function-wise Expense Subsidiary Ledger	
Journal Book	
Ledger Book	
Cheque Issue Register	
Trial Balance, Income & Expenditure Statement	
Balance Sheet	
Bank Reconciliation Statement	

Roles	Users
Cheque Dishonour Report	Intranet, MSC
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	

Audit Module

Roles	Users
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
Exceptional Reports (w.r.t. deletion of records, adjustment entries, etc.)	Accounts, Other Modules

4.15 Kakinada City Network System:

4.15.1 Overview

With technology being a key driver for implementation of Smart Kakinada City initiatives across the *Kakinada City*, a robust network is one of the key foundational requirements on which future ICT based 'Smart' initiatives shall be designed and built. Accordingly, Authority has decided to establish a Kakinada wide network backbone infrastructure that shall act as the backbone for effective implementation of smart Kakinada initiatives across the *Kakinada City*.

The provisioned network backbone infrastructure shall be designed in a manner which shall be capable of carrying out all the key services that shall be implemented in due course under smart Kakinada initiatives. The Authority wishes to establish a dedicated and secured fiber optic network backbone across the *Kakinada City*.

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

a. Connectivity – Network that interconnects citizens, government, business houses and other communities.
b. Smartness – Network would allow better management and control to offer richer and smooth application usage experiences.
c. Secure, private and resilient – Network built considering security standards and best practices with stability in bandwidth provisioning and resilient
d. Efficient – Network that is capable to deliver the envisaged bandwidth and related services
e. Scalable – A network that can scale up to cater all the bandwidth requirements for deployment of future smart Kakinada City initiatives

Multiprotocol Label Switching (MPLS) based network or better is expected to be provisioned for the backbone network: The network backbone is expected to help the *Kakinada city* to build a converged network, bringing together different Kakinada management vertical solutions on a single foundational network infrastructure. The converged network shall facilitate information exchange between various resources and applications across different domains. It is proposed to be an end-to-end platform enabling delivery of varied services for citizens. Key objectives envisaged are to provide:

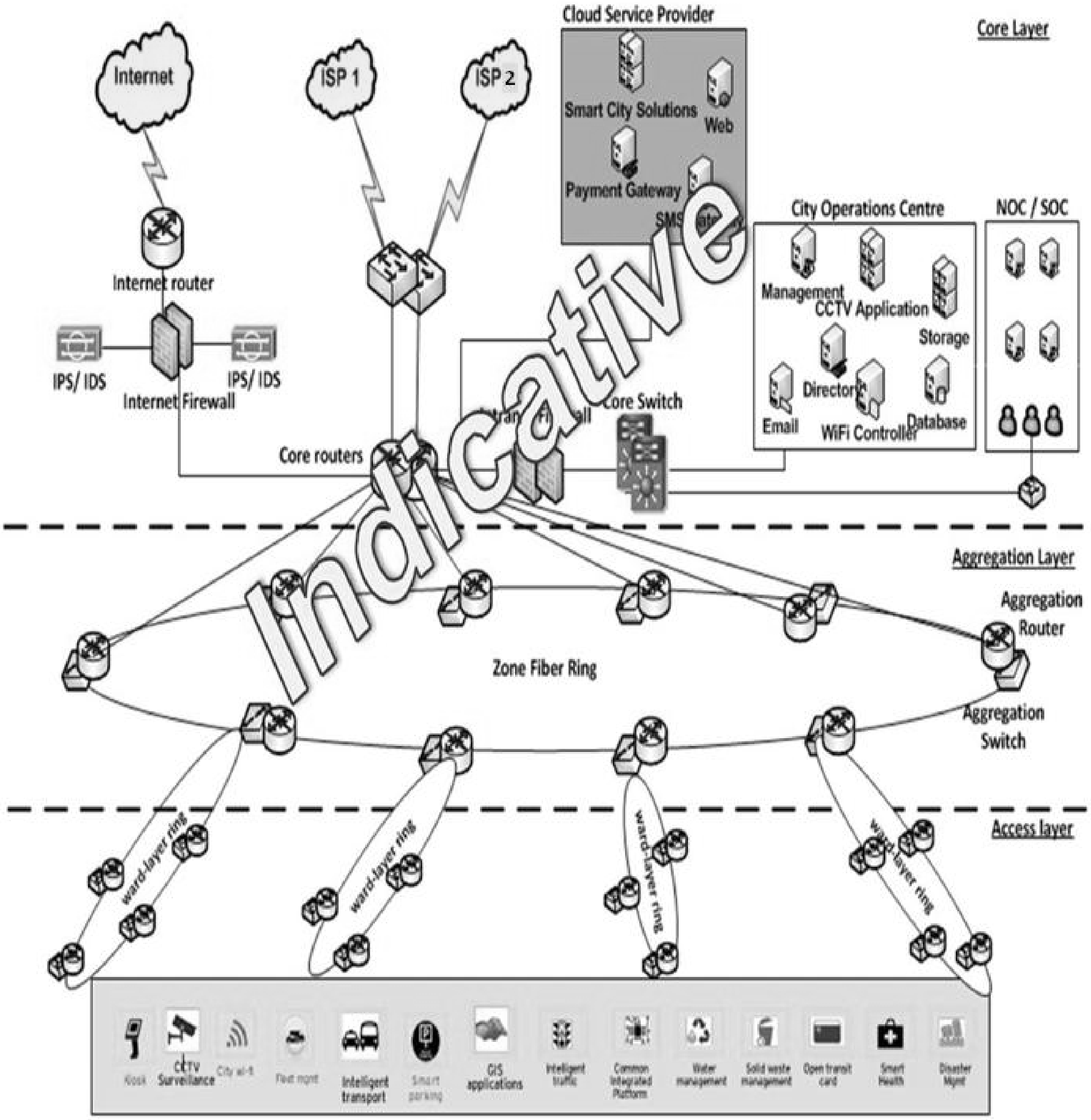
a. IP connectivity that shall enable the citizens to avail varied services under smart Kakinada initiatives
b. Wired and wireless, scalable, and highly secure network platform
c. Data management framework to help enable data collection, organization, and sharing
d. Adoption and usage of distributed computing and storage services, location based services and security services

4.15.2 Solution requirements

A.Functional design

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

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



The envisaged layers of the Kakinada City Network Backbone are:

a. **Core Layer:** The Core layer forms the backbone of the entire network which consists of Computing devices, storage, application software, links and connectivity to be established at the Command Control Center (CCC) and Kakinada City Operations Centres (KCOC). This layer shall enable all applications hosted at CCC and KCOC to be accessed over the backbone for consumers and users. Core layer shall form the point of aggregation for all the traffic coming from the Zonal layer and beyond.

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

c. **Access Layer –Ward Level**: The Access layer shall be formed at the wards of authority. All the wards in the respective zone shall form individual rings to establish redundancy. There can be multiple rings within the respective zone. e.g. if there are 10 wards in a given zone, then two rings comprising of 5 wards each can be created. These two rings shall ultimately connect to the respective zonal Point of Presence (PoP). The access layer shall enable the smart Kakinada solutions to connect to the network backbone. The aggregation switch of the respective smart Kakinada City solution shall tap on the respective access layer devices.

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

e. Various locations for deployment of above layers:

#	Item	Deployment location
1	Core layer	Command Control Center and Kakinada City Operations Center.
2	Aggregation layer	Identified aggregation points as mentioned in ANNEXURE V. These are mostly Authority zonal offices and tentatively identified government office buildings. A minimum of 10 such aggregation points are being considered. SI may estimate and propose the number of aggregation points as per requirements.
3	Access layer	Aggregation points to be identified by SI based on network load and geographical coverage. A Minimum of 10 rings for access layers to be considered by SI. These may overlap in order to provide required redundancy.
4	Services layer	The services layer is considered to be the edge locations/area where the smart Kakinada City solutions shall be deployed like: • Kakinada City Surveillance System • Kakinada City Wide Wi Fi connectivity • ICT based Solid waste management • Smart Lighting • Smart traffic • Smart Parking • Solar Energy based Environmental sensors • e-governance

Key services which shall be provisioned under various layers:

1. Monitoring and Management – The monitoring and management layer shall be provisioned centrally from core layer. Centralized management of infrastructure resources shall be implemented in core, aggregation layer, zonal layer and ward layer. All key services that shall be provisioned for the users such as –
   a. Kakinada City wide Wi Fi connectivity
   b. CCTV surveillance
   c. All other Smart Kakinada City solution initiatives
2. Network Operations Center (NOC): The NOC shall consist of two layered network:
   a. Core layer: This shall monitor all the infrastructure devices (Router, switches, firewall, bandwidth etc.) that are kept in core layer, aggregation layer along with key services which shall be provisioned in due course

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

3. Configuration and change management: Configuration shall be managed from core layer for all the devices on the network. For any changes applicable, based on the type/severity/complexity of change, the changes should be proposed with due justification and to be implemented upon approval from the Authority.
4. The proposed solution shall be scalable in nature to host all key services under smart Kakinada
5. The proposed solution shall have redundancy built at each layer
6. The proposed solution shall be capable of allowing enough redundancy built at fiber as well as at infrastructure level
7. The proposed solution shall be ready to scale up both horizontally and vertically
8. The proposed solution shall be ready in all respects where it is envisaged by Authority to make use of this infrastructure under different revenue models under its long term vision.
9. The solution shall meet demands of bandwidth needs for all the procured and planned smart Kakinada City solutions
10. The solution shall easily integrate with Wi Fi subsystem that shall be connected on the same backbone infrastructure.
11. The solution shall be ready in all aspects to host FTTX model in near future to provide voice, video and data services over fiber

Fiber backbone infrastructure is an important component of the entire smart Kakinada City initiative that shall enable the delivery of all the key and important services to be made available to its citizens with seamless access. Network backbone infrastructure shall comprise of dark fiber, setting of various points of presence (PoP) that shall be established across Kakinada City and cover all zones and wards. The fiber shall be further utilized at access/ward layer for services to be enabled as and when required.

B. **Key requirements,** need to be fulfilled by the SI, while carrying the activities are provided as below:

1. **Route Survey & Network Design Preparation**:
   a. The SI shall prepare the route map & network design and submit the final route maps and network design to the Authority for its approval.
   b. The bidders are advised to make a detailed survey and familiarize themselves with the soil and terrain so that the rates quoted shall take all factors into consideration.
2. **Fiber Implementation:**

   Supply, delivery to site, unloading, storing and handling of 24 Core Fiber drums along with fittings and associated items as required.

   a. All fittings, accessories and associated works for proper and safe installation of fiber assets to be taken into consideration by the SI
   b. Laying, jointing, live line installation, testing and commissioning of all optical fiber and its accessories
   c. Training of Engineers/linesmen, both in supplier’s premises and at site, in the installation, operation and maintenance of the optical fiber cables.
   d. The estimated fiber optic cable length requirements to be indicated in the Bill of Material (BoM) and to be reflected in the Price Schedule.

Note: The SI shall be paid for the actual quantity supplied and installed at site. The measurement for quantity to be paid shall be based on horizontal route length of the optical fiber cable (OFC) laid and the approved unit price quoted by the SI.

3. Core Backbone

a. The core backbone shall be established using 24 Core Optical Fiber Cables.

b. The core architecture shall be established maintaining high level of redundancy and no single point of failure.

c. Two cores in each laid OFC shall be redundant for future scalability and maintenance activity.

d. The maximum fiber distance between Core and Zonal layer shall not exceed 8 Kms

e. Adequate loop of 10 to 15 meters of OFC shall be kept excess on junctions wherever applicable.

f. There shall not be more than one Splice, Joint closures installed between two (2) locations, during hand over of Network to Authority.

g. All the 24 cores shall be spliced & joined in the Core Backbone.

h. The color code shall be uniformly followed across the Core ring, zonal aggregation ring & ward ring.

i. The core shall adhere to ITU-T G.655 standards for Non-zero dispersion shifted Metal-free unarmored optical fiber cable conforming to TEC specification GR/OFC-07/02. Jul 2007 or latest and the raw material used in its manufacture will conform to TEC Specification TEC/GR/TX/ORM 01/04.

4. Zonal Aggregation Backbone – Ring Topology

a. The Aggregation rings shall be established using 24 Core Optical Fiber Cables.

b. The Zonal Aggregation architecture shall be formed using ring topology.

c. Two of the cores in each OFC shall be redundant for future scalability and maintenance activity. These two spare cores at Zonal Aggregation Backbone shall not be used for any other purpose apart from the stated.

d. Adequate loop of 10 meters of OFC shall be left on junction wherever applicable.

e. There shall not be more than one Splice Joint closures installed between two aggregations points during hand over of Network to Authority.

f. All the 24 cores shall be spliced & joined in the Zonal Aggregation Backbone ring.

g. The maximum fiber distance between Zonal layer shall not exceed 12 Kms

5. **Ward (Access) Backbone – Ring Topology**

a. The Ward rings shall be constructed using 24 Core Optical Fiber Cables.

b. Multiple Ward rings shall be created for the zones that ward is falling under for eg. If there are 10 wards in a zone, two rings of 5 wards shall be created.

c. The Ward Aggregation architecture shall be formed using ring topology

d. Two cores in each OFC shall be redundant for future scalability and maintenance activity and these cores at the Ward Backbone ring shall not be used for any other purpose apart from the stated.

e. Adequate loop of 10 to 15 meters of OFC shall be left on junction wherever applicable.

f. There shall not be more than one Splice Joint closures installed between two aggregations points during hand over of Network to Authority.

g. All the 24 cores shall be spliced & joined in the Ward Backbone ring.

h. The access layer shall be extended using the lit fiber which shall be used to allow all the key services to pass through the network backbone. The access point, CCTV surveillance system and other smart Kakinada City components etc. shall be plugged into lit fiber to enable the services to users.

4.15.3 Scope of Work

A. Planning and designing of Network backbone architecture

I. Site survey and studying of available infrastructure

SI shall carry out site survey of locations as identified for implementing various smart Kakinada initiatives mentioned in the RFP and also potential locations for future initiatives based on the discussions and approval from the Authority.

a. In order to optimize the existing infrastructure facilities and to ensure cost effective project execution, it is necessary to scan the building at the authority zonal offices where the OFC can be terminated along with relevant IT equipment. For this purpose, the following order of preference shall be followed:
   - Housing of the optic fiber equipment in Authority zonal office building
   - Housing of the optic fiber equipment in government owned building
   - Housing of the optic fiber equipment in privately owned premises on wayside (these locations have to have prior approval of the authority).
   - Route through which the fiber cable shall run through the building in a secured manner

b. However, the recourse to utilize any of the above mentioned alternatives shall be made subject to:
   - Expenditure on addition/alternation necessary to make the room suitable for housing the optic fiber equipment shall be much less than cost of construction of new room at the appropriate site for Optic fiber equipment.
   - The total area shall be sufficient to accommodate the layout required.
   - The location of building to be considered in a manner which is close to the cable route to avoid extra cable length.
   - Power supply is made available and preferably standby power is also made available. The electric meter shall be in the name of the Authority; however, the provisioning and the electricity expenses to be borne by the SI during the contract period.
   - The site shall be higher than highest flood level of that place.

c. In case the existing building for wayside location is not available, a new optic fiber equipment building for wayside location shall be decided with the following considerations.
   - Site shall be close to the key locations identified for smart Kakinada City initiatives.
   - Staff quarters and other residential building/restaurants, tea stalls shall not be close by
   - Site shall be at an appropriate ground level
   - Site in-between roads to be avoided
   - Preferably the site shall be on the same side of the road as the route of optic fiber cable
   - Consideration for road access to site
   - Sufficient open space is available for storage of the equipment
   - Security of the equipment shall be the responsibility of SI at the respective site.

d. Ground Probing Radar (GPR) may be used to identify the cable duct path and the proposed aggregation points.

e. For maintenance purposes, 5% additional pipe provision may be considered for estimation.

f. Indicative measurement of lengths of cable route along with the details of rail/road crossings, culverts, causeways etc. may be recorded in the detailed survey register. The probable location of joints, terminations and leading-ins may also be decided and marked on the road map.

g. Based on the assessment undertaken, SI shall undertake a detailed and comprehensive network architecture development of the entire Smart Kakinada City solution covering all the locations in *Kakinada City*, IT and physical infrastructure in line with the overall objective and requirements of the project. SI shall identify the space required for setting up the network infrastructure at each of the location.

h. SI shall be required to undertake the GIS based survey to design the OFC route planning and network topology and share the same with the Authority. SI can make use of the publicly available data and tools such as Google Maps, ArcGIS, NIC developed maps, etc. However, the ownership of the accuracy and validation of the data map information shall be with the SI.

i. The network architecture development exercise shall cause development of the following:
   i. Detailed WAN and Network architecture covering all locations
   ii. Detailed Fiber layout along with details of fiber to be laid by using existing authority's fiber ducts (if any) or by laying new Fiber ducts
   iii. Detailed Network solution and deployment architecture covering the central infrastructure at Central Command Centre, Kakinada City Operations Centre, IT architecture for Kakinada City Surveillance, Kakinada City wide Wi Fi connectivity and other smart Kakinada City solution components.
   iv. Solution required for managing/monitoring the complete Network Backbone.
   v. Detailed information security architecture to ensure data privacy as well as security

j. SI shall prepare a Network architecture that includes all of the above along with other design elements like data standards, technology standards, interoperability standards, security architecture and other such guidelines/standards as shall be required for developing a state of the art Smart Kakinada City solution. This shall be prepared in active consultation with Authority.

k. SI shall factor inclusion of various Govt. offices and their location, bandwidth requirements, security, LAN/WAN protocols, network topology for each of the Smart Kakinada City solution its utilization and allocation of bandwidth etc. shall be taken care of at the time of designing the overall network architecture.

l. SI shall be responsible for gathering the Bandwidth and LAN connectivity requirements at junctions, Data Centers, Command Centers, and observation centers. The LAN connectivity may involve setting up the structured cabling, commissioning of active and passive components for operationalization of the Smart Kakinada City System.

m. The actual bandwidth requirement and storage parameters required to meet SLAs should be calculated by the SI and the same shall be clearly proposed in the Technical Bid with detailed calculations for all smart Kakinada City solution components. Kakinada *City* also requires the SI to meet the parameters of video feed quality; security & performance and SI is required factor the same while designing the solution.

n. SI shall also consider the terrain, topography, climatic conditions etc. while designing the network architecture.

o. The Network Architecture once approved shall be base lined either in part or in whole and the Authority shall institutionalize the processes for Architecture Change management to undertake any change in the respective location, as required during the contract phase.

p. Designing IP Address Schema
   i. The SI shall design suitable IP Schema for the entire Network Backbone including Central Command Centre, Kakinada City Operations Centre, Zonal offices, ward locations, smart Kakinada City solutions and interfaces to external systems/ network. The SI shall ensure efficient traffic routing irrespective of link medium.
   ii. The SI shall maintain the IP Schema with required modifications from time to time within the scope of the project.

II. Preliminary fiber route survey

Preliminary survey shall be carried out for finalizing the drawing for the route of optical fiber cable as part of project planning and execution.

Following main items of work shall constitute this survey:

a. Selecting the route in general
b. Deciding the number of drop and insert locations
c. Deciding the size and assessing the length of cable required
d. Working out the requirement of circuits that are to be provided in the cable
e. Working out the requirements of heavy tools and plants depending upon nature of the territory, availability of roads alongside etc.
f. Assessing the special problems of the section such as type of soil, long cuttings, new embankments, water logged areas, types of major bridges, major yards etc.
g. Collecting details of the existing telecommunication facilities and the additional requirements for electrification and preparing tentative tapping diagrams
h. Assessing the number of road crossings and other protective works required to be done
i. Avoiding as far as possible laying of cable too close to a newly built road
j. Avoiding the toe of the embankment adjacent to the cultivated fields
k. Avoiding burrow pits and areas prone to water logging
l. Avoiding heavily fertilized soils containing acids, electrolytes and decomposable organic materials promoting bacterial activity
m. Avoiding proximity to chemical, paper and such other industries which discharge chemically active effluents
n. Avoiding large rock cuttings, routes of existing cables and areas difficult to approach
o. Deciding carefully the cable route approaches to cable huts to avoid built up areas including those areas where building, etc. are likely to come up in future
p. Determining composition of the soil which may affect corrosion, etc. on the cable and special protection required for cable
q. Working out requirement of transport vehicles like jeeps, lorries, motor trolleys, etc. for execution of the work
r. Avoiding side of the alignment which is likely to be affected due to addition/alteration of earth work/supply structures

III. Preparation of cable route plan and tapping diagrams

The cable route plan shall indicate the route with respect to the main road, that is, whether the route along the main road is on both sides and right side of the main road when facing a particular direction in case of single line section.

Selection of the Cable Route

Generally, the terrain conditions on the two sides of the road vary to such an extent that the cable route on one side of the road has a distinct advantage over that on the other side. While operating on the principle, it shall be borne in mind that frequent track crossings are not desirable.

In addition to the above, the following points are also needed consideration:

a). Avoiding underground structures, signaling cables, power cables, pipe lines, etc.
b). Avoiding laying of cable on the side of the drains in built up areas which are difficult to lay
c). Taking the cable route preferably through the bed of small culverts where water does not accumulate instead of taking it over the culverts
d). Avoiding termites/rodents infected areas
e). Identification of site locations for zone and ward level aggregation points

IV. Laying of Optical Fiber Cable

a. SI shall employ industry leading practices for laying fiber for Authority's existing ducts and new ducts.
b. The Authority shall facilitate the SI to get all the necessary permission(s) for fiber laying including the Right of Way. SI shall be responsible for coordination for all the activities in this regard.

c. Before carrying out the actual fiber/duct laying process, the SI is encouraged to carry out a detailed survey based on the outcomes of the preliminary survey carried out earlier. The purpose of the detailed survey is to undertake closer study of various existing telecommunication facilities to work out exact requirement of materials for different items of work to finalize all the drawings and site plans required for the execution of work as also to examine the details collected during preliminary survey and to incorporate necessary changes/modifications, if any.

d. The following are the main items of work that shall constitute the detailed survey:

   i. Closely examining the proposed cable route and prepared cable route plans
   ii. Siting of cable hut buildings and preparation of site plans
   iii. Siting and preparation of site plans for buildings required for the execution of the work, as offices at different stations, store go-downs
   iv. Siting of areas for loading/unloading of cable drums and siding facilities for the EMVs (Engineering Materials Vehicles) for the project
   v. Preparation of the material schedule required for different protective works
   vi. Arranging isolated components circuits to be provided in the cable
   vii. Investigation of special problems, if any, of the section and finding out proposed solution thereof

e. On Ducted Routes: Optical fiber cables may be laid through the existing ducts wherever the concrete ducts are available. As far as possible the cable may be diverted to the new ducts laid subsequently. When the cables are laid in ducts, no particular depth is prescribed. End of the ducts shall be properly sealed and necessary protection by way of W.I. pipe/RCC pipe shall be provided at the entry and exit of the duct till the cable is buried to a depth of 1.5 m.

f. On Non-Ducts Routes: PLB pipe laying shall be done as per the approved detailed survey report

g. SI is expected to put in practices for precaution against damage by Termites & Rodents. In the rodent prone areas, Optical Fiber cable joint closures shall be applied with BHC 10% dust (Benzene Hydro chloride 10%) to prevent rodent & termite damage. The method suggested is “BHC” 10% dust of 1 kg shall be mixed in an approximate 2 kg of sand and applied around the optical fiber cable joint enclosures

h. Cable laying is proposed either by traditional Cable pulling method or by Cable blowing method

i. Technical Specifications of HDPE Pipe. The HDPE pipe will conform to TEC specification GR/CDS and latest amendments thereof or better. The HDPE pipe used will be of 40 mm outer diameter with minimum wall thickness of 3.5 mm.

j. To reduce the friction between the cable and HDPE, a suitable lubricant may be continuously applied with a sponge to the cable surface during pulling. The standard lubricants with low frictional coefficient may be used. Telecom Duct may be adopted. Telecom Duct is an advanced pre-lubricated duct system. Lubricants are built in to a durable polymer base. Duct has a low coefficient of friction and the built in lubricants do not diminish with age. SI is expected to choose the industry’s best practices while carrying out the above mentioned tasks.

k. Following types of techniques shall be used for splicing of fibers: -

   i. Mechanical Splice - This is done by aligning the axis of the two fibers to be joined and physically hold them together.
   ii. Fusion Splicing - This is done by applying localized heating (i.e. by electric arc or flame) at the interface between the butted, pre-aligned fiber end, causing them to soften and fuse together.

l. Mechanical splicing shall be used for temporary splicing of fibers or where fusion splicing is impractical or undesirable.

m. At all other locations and during initial installation of optic fiber cable, fusion splicing shall be adopted.

n. Authority may choose to carry out an acceptance test for fiber that has been laid. In either case, SI is expected to carry out an independent review of the fiber/duct that has been laid for the purpose of creating network backbone. Such inspection reports shall be submitted as supporting documents while raising invoices. Authority may ask the SI to carry out this sample test from a third party agency. Cost of such tests shall be borne by the SI.

o. In case any deficiencies observed in the laying of fiber/duct by SI, SI is expected to promptly correct the same at no extra cost to the Authority.

p. For rectification of faults, etc. special kits shall be used for opening of the joint

q. SI shall be liable to pay any penalties imposed while carrying out work. Authority or any of its representatives shall have no liability arising from penalties including but not limited to penalties for causing inconvenience to the public, penalty for cutting/damaging the old cable of authority or other service providers, penalty for damaging any other utilities, among others.

r. Termination joint for optic fiber cable is provided in the cable hut for terminating the outdoor optic fiber cable of both the sides, splicing through fibers, connecting fibers to pigtails for connection to optical line terminal equipment, etc. SI shall choose appropriate procedure for installation of termination joint box based on the type of joint enclosure. The installation manual shall contain the step by step procedure for installation. After the cable is laid and splicing is complete, measurements as per the proforma indicated herewith shall have to be prepared and maintained.

Section		**Distance**	**Cable Length**	**Fiber No.**	**Loss in dB**		**Remarks**
From	To				1310 nm	1550 nm	

The end to end loss shall not exceed 0.25db/Km at 1550 nm and 0.40 db/Km at 1310 nm

B. Network backbone infrastructure management - Commencing network backbone infrastructure management including handover to Authority and maintenance team

List of items to be handed over to Authority/designated authority before handing over the respective section/location for maintenance of optical fiber communication system

a. The Cable Route Plan in electronic form (in kml file format on a CD) preferably using AUTOCAD and Google maps. Distances from fixed reference structures like centre of track, OHE mast, bridges, culverts, etc. shall be indicated in the route plan for easy reference in future.

b. The Fiber Distribution Plan

c. Measurements of Optical Parameters which include sectional losses splice wise losses, records of dispersion measurements (in case of long haul systems) shall be handed over to the maintenance organization.

d. SI shall prepare maintenance schedule for fiber optic system. Reports on adherence to the maintenance schedule shall be submitted as part of SLA compliance along with quarterly invoices. This maintenance which shall include but not be limited to following areas:

    i. Power supply equipment

    - Maintenance of Charger and In/Out voltages and currents
    - Checking of fuses and terminations & Earthing

    ii. Optical fiber cable

iii. Cable route
   - Integrity of cable route
   - Protective works on bridges & culverts
   - Cable route markers
   - Earthing of sheath of cable

iv. Periodical line-up consisting of
   - Tx/Rx optical power
   - Pulse mask for all digital interfaces
   - G821/G823 tests on 64KBPS/2MBPS for 10 days
   - Loss measurement with optical source & power meter
   - Measurement of order wire performance circuits.

C. Alternate Network Connectivity Provision

The SI has the option of sourcing the bandwidth from the telecom service provider. Connectivity infrastructure will connect the project sites like DC, DRC, CCC, Kakinada City operation center, Camera Locations, Access points and other smart Kakinada City components etc.

The SI will undertake the following:

a. The coordination with Telecom Service Providers to ensure last mile connectivity of all project sites.

b. LAN within all Project sites including but not limited to IP addressing scheme, physical cabling, router/switch configuration, V-LAN configuration, load balancing configuration, and fail over mechanism. The SI should coordinate with the local department offices while designing and installing the LAN.

c. All networking equipment required in provisioning the LAN/WAN connectivity to meet the requirements of the Project is also to be provided by the SI as part of this RFP **scope.**

The SI to ensure that while sourcing the bandwidth from the telecom service provider the deliverables as mentioned in this section 1.1 (as in case of laying dedicated fiber network) are adhered to and the necessary design to be adopted by the SI accordingly under approval from the Managing Director, KSCCL, Kakinada.

4.16 Kakinada City Wi Fi Connectivity

4.16.1 Overview

In a society with a high demand for digital connectivity “on the move”, there is an increasing demand for public Wi Fi services, which are required to be made widely available. Understanding this need, Authority intends to provide public Wi-Fi services at identified locations across the *City.* These locations shall include Market Places, Government Offices, Recreation and Tourist Spots such as parks & lakes, Educational Institutes, Holy places, etc.

The Kakinada City wide Wi Fi connectivity shall leverage Kakinada City Network Backbone (which shall be made available across *the City.* SI shall extend the last mile connectivity through Kakinada City Network Backbone to Kakinada City wide Wi Fi locations over fiber. The SI shall install access points and lay the fiber cabling at identified locations along with implementation of access points and provide maintenance support to Authority or its authorized entity. The selection of access points shall be done on the basis of density of users, geographical coverage and in consultation with Authority or its designated agency.

To start with, access points shall be provisioned at identified locations. Based on demand new Wi Fi locations can be added. The access points shall be implemented in controller based model where access points shall be managed by using wireless controller that shall be positioned at Data center. The proposed solution shall include access points and related infrastructure as per specifications mentioned in the RFP. However, the standards of design and services should (a) at least comply with the published e-Governance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and (b) be of leading industry standards and /or as per standards mentioned at Annexure –XI.

SI is expected to procure bandwidth services till the time Kakinada City network backbone is created.

SI shall conduct the survey and design the Wi-Fi setup at each location to accommodate the users' bandwidth needs and requirements. Profiling of users and appropriate policies shall be pushed from Data center. Wireless controllers shall also be integrated with AAA (Authentication, Authorization & Accounting server) to properly manage the policies that may be required for different user types. Access points shall negotiate using Service Set Identifier with controller. The controllers register the access points and accordingly allow the access point post checking with AAA server.

SI shall supply, install, commission and maintain the access points and related infrastructure (for the entire duration of contract period). Based on need, SI shall be required to supply additional access points as per the unit rate quoted in the financial bid.

4.16.2 Solution requirements

Key expectations from the system include:

a. The network shall support user devices with 2.4 GHz as well as 5.8 GHz frequency band at the same time
b. The Kakinada City Wide Wi-Fi network should be manageable from a central location at Kakinada City operations centre through the wireless management system. The management system shall support unified wired and wireless network management.
c. It shall be possible to configure and manage access points (APs) remotely through a wireless controller.
d. System shall support multiple VLANs to support users with different privileges.
e. The system should be designed for scalability and allow future expansions in terms of subsequent project phases, increased user density and geographical coverage.
f. Data communication between devices shall take place in encrypted form to ensure end-to-end security of user information/ data with requisite security standards.
g. The system should be designed for multiple authentication mechanisms
h. The system shall support user authentication and one time OTP based registration, thereafter user shall login through chosen username and password.
i. Every user shall get access to only those services for which they are authorized.
j. The system should be capable of Rule based Access Rights.
k. The system should have centralized billing and authentication system wherein profile for each individual user shall be created.
l. Users shall be able to manage their account by subscribing/renewing the packages on the self-service portal.
m. New users should be given the free access of say 50/100 MB to use limited services (for better interaction with the Government and availing citizen services) for subscribing the available plans.

The access points may be deployed outdoor or indoor depending on the requirement of the Authority or its assigned agency. The implementation of these access-points shall be carried out on the basis of feasibility of access-points at each location and in consultation with Authority.

4.16.3 Scope of Work

The SI shall be required to carry out following activities:

1. Survey of the defined locations to ascertain number of Access Points and their positioning to ensure maximum coverage and excellent signal strength. This shall be done in consultation with officials assigned by Authority or its authorized entity

2. Supply, installation, integration, testing, commissioning and maintenance of all products required for enabling 24x7 Kakinada Wi Fi services at identified locations. These include but are not limited to IT, telecom, networking, peripheral hardware and software products and applications.
3. Leverage Kakinada City Network Backbone infrastructure that is being created for *Kakinada City*. However, till the time Kakinada network backbone is commissioned by the SI, the SI needs to procure bandwidth as a service in order to meet requirements as defined within service level agreement. Authority estimates provisioning of Kakinada Wi Fi services at [No. of locations] locations across the Kakinada with 10 Mbps bandwidth at each AP level. However, in times to come, Kakinada Wi Fi locations may scale up, hence SI needs to provision for the network bandwidth accordingly.
4. Development and implementation of billing and accounting software for e-recharge and accounting for the service revenue.
5. Multiple payment gateway integration required so subscribers can make the payments using online/ offline mode, including prepaid mobile balance & wallet applications.
6. Advertising platform integration -AAA to support advertisements from multiple parties.
7. SI shall also be responsible for:
   a. Providing Technical manpower, for the contract period from the date of acceptance, to look after the day to day management of services related to Wi-Fi facility management. These services shall include:
      i. Providing connectivity to user devices as per Wi-Fi access policy,
      ii. Satisfactorily handling all the issues related to connectivity, performance and security.
   b. Edge or street level network including access network architecture leveraging Kakinada network backbone
      i. Planning and design of the Edge network architecture (access controllers, backhaul connectivity, routers, switches, fiber, junction box, UPS, etc.) to meet the technical, capacity Kakinada and service requirements.
      ii. Planning for high availability, reliability and redundancy of the access network elements as per requirements stated in the SLA.
   c. Kakinada city Wi-Fi Locations
      i. Authority shall be providing of Access Point locations
      ii. Commissioning & deployment of Wi Fi solution
         a) SI shall be responsible for design and RF planning based on the locations identified by Authority.
         b) SI shall be responsible for installation of Access Points and related equipment at Wi Fi locations
         c) SI shall be responsible for providing and executing cabling, testing etc.
   d. SI shall be responsible for design and engineering of all the network components to meet capacity Kakinada requirements
      i. Network shall be designed keeping in view the peak load conditions.
   e. The network should support Low Power WAN. The few common technical specifications/parameters of similar networks like LoRa, LoRa WAN, Sigfox, Weightless, Narrow Band internet of things (IoT) and likewise. The specification towards LPWAN should be:
      - Minimum 5-10 km of communication range
      - Higher capacity Kakinada towards number of nodes that can communicate
      - Long battery life
      - Low interference
      - Operational into the free wireless band

- Secure bi-directional communication
- Localisation services
- Ability to integrate with backend Cellular/Wi-Fi network
- Longer battery life for end-devices/nodes

f. Equipment and network upgrades, support and maintenance for the contract period
    i. SI shall provide local support at each zone for repair and maintenance of all equipment, cabling and connectivity provided at the Kakinada Wi Fi locations
    ii. SI shall be responsible for periodic updates of all equipment, cabling and connectivity provided at the Kakinada City WiFi locations

g. Set up Wi-Fi network across locations proposed in phased manner

h. Procurement, planning, design, installation, commissioning and support of all end point equipment (IT and non IT) required to set up Wi Fi locations.

i. Providing adequate security mechanisms in Kakinada Wi Fi service equipment to prevent unauthorized access or interfaces to services, calls, protocols and data.

j. Providing complete network diagram including detailed technical documentation, survey, drawing and detailed Project Plan for all the locations mentioned.

k. Kakinada Wi Fi management: Kakinada Wi Fi setup shall be monitored and managed at core layer. The Kakinada Wi Fi access points shall be provisioned in client server mode where controller of the Kakinada Wi Fi system shall be placed at core layer and all access-points based on the feasibility shall be implemented at ward layer. All the key services available for citizens shall be catered using Kakinada Wi Fi access.

l. Ensuring compliance with all Regulatory and Legal guidelines issued by Department of Telecommunications, TRAI and Government of India from time to time. At no point Authority or its authorized entities shall be responsible for any non-compliance on account of non-adherence by the SI.

m. SI should plan usage analytics.

4.17 Kakinada City Surveillance System

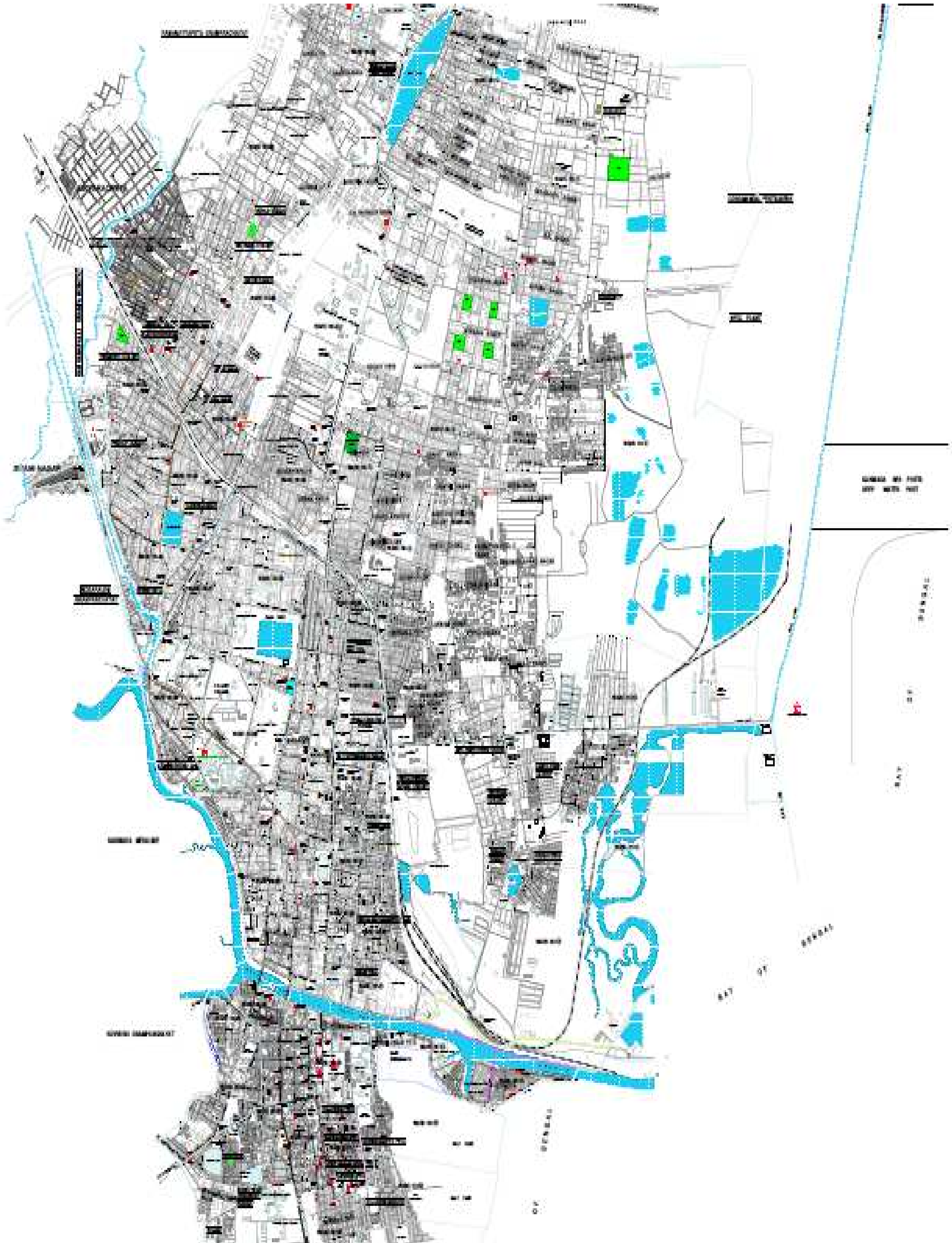
4.17.1 Overview

Protecting citizens and ensuring public safety is one of the topmost priorities for any Government agency. It requires advanced security solutions to effectively fight threats from activities of terrorism, organized crime, vandalism, burglary, random acts of violence, and all other forms of crime. CCTV based video surveillance is a security enabler to ensure public safety. Government of [State], under the smart Kakinada initiative, intends to implement a holistic Kakinada City Surveillance System in Kakinada Police Jurisdiction limits of *Kakinada city*.

4.17.2 Geographical Spread

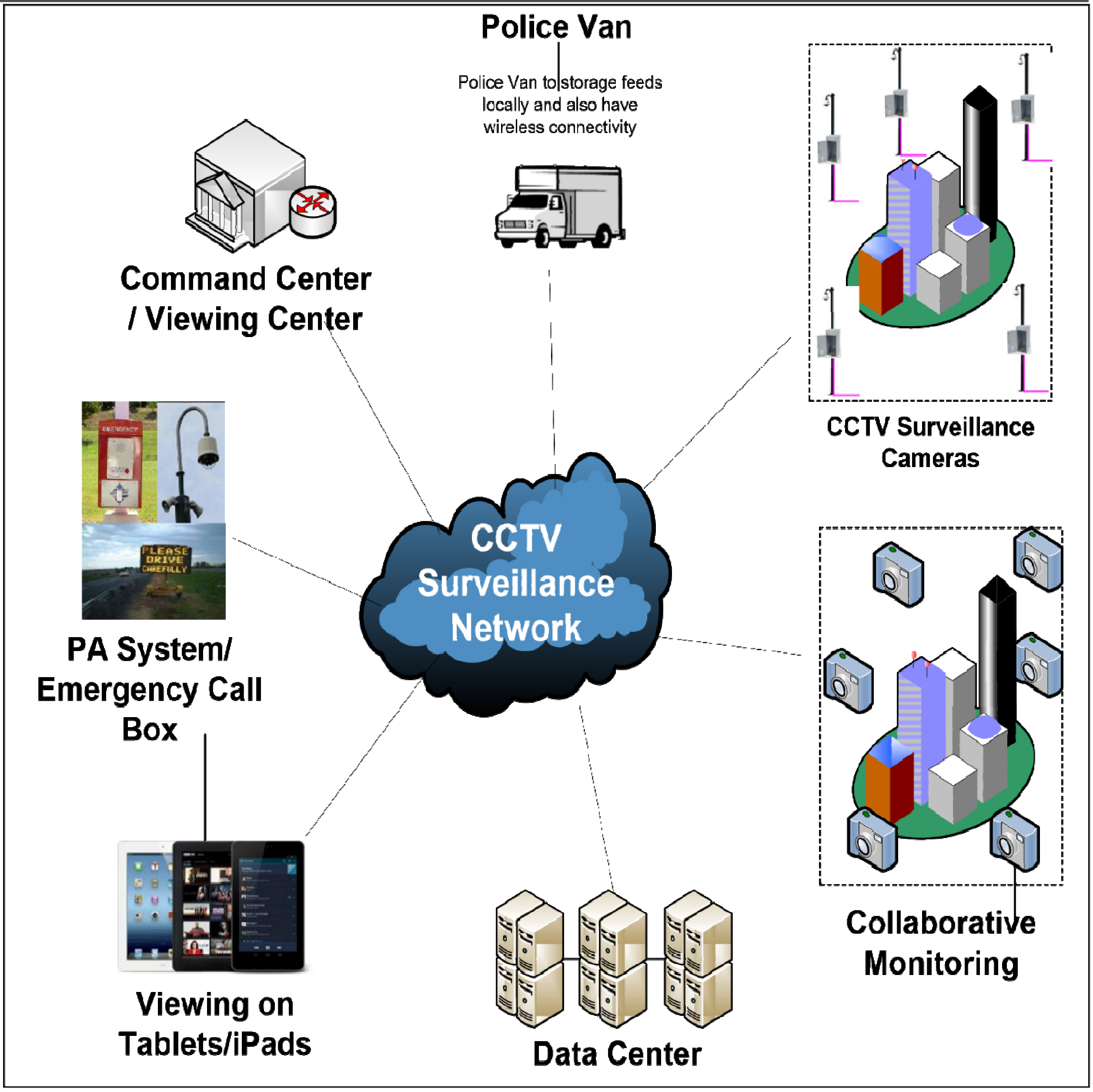
The following map represents the Geographical spread of the area and zone wise distribution of police jurisdictions. This includes the *Kakinada city* Municipal Corporation limits.

Kakinada city Municipal Corporation Map



4.17.3 City Surveillance

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


Police Van
Police Van to storage feeds locally and also have wireless connectivity
Command Center / Viewing Center
CCTV Surveillance Cameras
PA System/ Emergency Call Box
CCTV Surveillance Network
Collaborative Monitoring
Viewing on Tablets/iPads
Data Center

Feed/Message to Police Van is optional

4.17.4 Solution requirements

The SI shall be responsible for Supply, Installation, Implementation and Operation & Maintenance of *Kakinada city* Surveillance System for a period of Five Years from the date of Go Live of the respective phase independently. The standards should (a) at least comply with the published e-Governance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and (b) be of leading industry standards and /or as per standards mentioned at Annexure –XI. The indicative requirement for SI is broadly categorized into following:

Category	Scope of Work
Min Surveillance System Infrastructure at field locations	Supply, install, implement and maintain: ▪ Full HD IP Pan–tilt–zoom camera (PTZ) Camera ▪ Full HD IP Fixed Box Camera ▪ Full HD IP Dome Cameras ▪ Thermal Camera ▪ Pole, Junction box, UPS, LAN switch, passive items, etc.
	1. Cameras to support ANPR 2. Cameras to support RLVD 3. Cameras with online FRS 4. Cameras to support analytics Other components: 1. Public Announcement System 2. Variable Messaging System 3. Drone 4. Mobile Surveillance Vehicle **Data retention period: 90 days**
Network Infrastructure	1. Between camera & aggregation point – Field location 2. Between aggregation points & Data center 3. Between Data center & command control center and Kakinada operation center. 4. Between Data center & viewing/monitoring center 5. Between drone ground station / mobile surveillance vehicle & Data center It is envisaged that the system shall leverage Network Backbone infrastructure that is being created for *the City.* However, till the time Kakinada network backbone is commissioned, SI is expected to procure bandwidth as a service in order to meet requirements as defined within service level agreement. The SI is also expected to migrate to the Kakinada Network Backbone within a month of operationalization of Kakinada backbone.
Data center	1. Supply & installation of IT Infrastructure including server, storage, network components and peripherals to handle 100% load along with provisioning for redundancy 2. Supply & installation of Non IT infrastructure like furniture, AC, and interior work etc. excluding civil work at the space provided by the Authority. 3. Set up of DR site with 100% redundancy of infrastructure.
Command Control Center	Supply & installation of IT & Non IT infrastructure like video wall, workstation, furniture, AC, and interior work etc. excluding civil work at the space provided by Authority 2. Supply & establishment of Mobile Command Control Center 3. Establishment of Forensic Investigation Room 4. Establishment of Dial 100 control room

Category	Scope of Work
Kakinada Operation Center	Kakinada Operation Center establishment at the identified location for viewing and controlling the selected field locations in a fully automated environment including:Supply & installation of IT & Non IT infrastructure like video wall, workstation, furniture, AC, and interior work etc. excluding civil work at the space provided by Authority
Surveillance System Applications	1. Video Management System (VMS) 2. Video Analytics (VA) 3. Red Light Violation Detection (RLVD) System 4. Automatic Number Plate Recognition (ANPR) System 5. Facial Recognition System (FRS)
Video feeds at few selected locations	SI is expected to provision for viewing of feeds at selected key police locations
Training/ Capacity Building	Technical & functional training to the designated officials on a continuous basis

4.17.5 Scope of Work:

A. Surveillance System Infrastructure at Field Locations

This Component covers planning & implementation of the Surveillance system comprising cameras and other field equipment at identified locations. Actual placement of pole & number of cameras at each location, type of cameras, fixation of height & angle for the cameras to ensure maximum coverage shall be done in consultation with the authority. A detailed survey shall be conducted, by the SI along with a team of Authority and the *Kakinada city* police, at each of the strategic locations. This survey shall finalize the position of all field equipment and the orientation/ field of view of the cameras. Appropriate field of view snapshot shall be taken by a handheld camera for future reference at the time of survey. The surveyors shall also finalize the approximate location of foundation for junction box and camera poles. The route for all the underground cable laying shall be finalized during this survey (wherever required). Every detail, finalized during the survey, shall be demarcated on an AutoCAD drawing by the SI and submitted to Authority in the form of a detailed site survey report along with other details for its approval.

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

1. Cameras (Fixed Box Cameras, PTZ Cameras, ANPR cameras etc.)
2. IR Illuminators
3. Local processing unit for ANPR / RLVD cameras
4. Switches
5. Outdoor Cabinets
6. Pole for cameras / Mast
7. Outdoor Junction box
8. UPS
9. Networking and power cables and other related infrastructure

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

B. Supply & Installation of CCTV Surveillance Infrastructure:

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

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

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

C. Installation of Poles/Cantilevers/Gantry

1. The SI shall ensure that all installations are done as per satisfaction of Authority.
2. For installation of variable message system (VaMS), CCTV Cameras, PTZ Cameras, public address system, etc. SI shall provide appropriate poles & cantilevers and any supporting equipment.
3. SI shall be required to supply, install, configure and integrate surveillance cameras at the identified locations and thereafter undertake necessary work towards their commissioning.
4. SI shall ensure that the poles erected to mount cameras are good, both qualitatively and aesthetically
5. SI shall use the industry leading practices while positioning and mounting the cameras and ensure that the pole / mast implementation is vibration resistant. Arrangements for bird scare spikes on top of camera shall be made to prevent birds from sitting on top of camera box.
6. The poles shall be installed with base plate, pole door, pole distributor block and cover.
7. Base frames and screws shall be delivered along with poles and installed by the SI.
8. In case the cameras need to be installed beside or above the signal heads, suitable stainless steel extensions for poles need to be provided and installed by the SI so that there is clear line of sight.
9. SI shall be responsible to undertake required structural analysis regarding the regulated load conditions and considering the respective wind load while installing the poles / cantilevers for cameras and Variable Messaging Sign boards
10. SI shall provide structural calculations and drawings for the approval of Authority. The design shall match with common design standards as applicable under the jurisdiction of Authority/authorized entity.
11. SI shall coordinate with concerned authorities / municipalities for installation.
12. Poles and cabinet shall be so designed that all elements of the field equipment could be easily installed and removed.
13. SI shall ensure that physical look of the installation area returns to neat & tidy conditions after installation of poles, cantilevers etc. The placement shall be designed keeping in mind the normal flow of vehicular traffic and pedestrian movement is not disturbed.

UPS for field locations

1. UPS shall serve as a backup for commercially available utility power at the intersections and shall ensure no-break functioning of all field components at each intersection in event of failure of utility power supply.

2. SI shall carry out a study and identify locations to provide UPS backup, depending upon power situation across Kakinada, to meet the camera and other field equipments uptime requirements.
3. SI shall install UPS at the identified intersections in secure, tamper-proof housing in corrosion resistant cabinets.
4. SI shall ensure that the UPS is suitably protected against storms, power surges and lightning.
5. SI shall provide UPS for efficient heat dissipation without air conditioning. It shall be able to withstand temperatures prevalent in the City throughout the year.

Outdoor Cabinets / Junction Boxes;

1. Each intersection shall be fitted with outdoor cabinets dimensioned to host all equipment necessary to operate enforcement systems and traffic surveillance systems as defined in this RFP.
2. SIs shall reserve additional room in the intersection controller cabinet to accommodate the future system requirements
3. The size of outdoor cabinet / Junction Boxes shall be sufficient to house all the system components, which may be installed at the intersection or nearby. Boxes shall be dustproof and impermeable to splash-water. They shall be suitable for the City's environmental conditions. They shall have separate lockable doors for:
   a) Power cabinet: This cabinet shall house the electricity Kakinada meter, online UPS system and the redundant power supply system
   b) Control cabinet: This cabinet shall house the controllers for all the field components at that particular location e.g. ANPR, PTZ, RLVD, Fixed cameras, etc.
4. Internal cabinet cabling shall be designed for an easy connection and disconnection of the equipment and power
5. The cabinets shall be of robust construction and shall include 3-point security-locking mechanisms to prevent unauthorized access to the field equipment
6. Temperature and Humidity Control: All enclosure compartments shall be equipped with a natural convection air circulation system via provision of air circulation filters that shall not require maintenance and shall allow free circulation of air inside the enclosures to prevent overheating as well as the build-up and effects of humidity and heat, without permitting the entry of elements that might endanger system operation.
7. SI shall ensure that all the hardware is placed inside the junction boxes that could withstand temperatures prevalent in City throughout the year.

Civil and Electrical Works

- SI shall be responsible for carrying out all the civil work required for setting up all the field components of the system including:
  a) Preparation of concrete foundation for MS-Poles & cantilevers
  b) Laying of GI Pipes (B Class) complete with GI fitting
  c) Hard soil deep digging and backfilling after cabling
  d) Soft soil deep digging and backfilling after cabling
  e) Chambers with metal cover at every junction box, pole and at road crossings
  f) Concrete foundation from the Ground for outdoor racks
- SI shall provide electricity Kakinada to the cameras through the aggregation point. Since this component has dependency on approval from local authorities, it is recommended that SI plans this requirement well in advance & submits the application to the concerned electricity Kakinada distribution agency with requisite fees, as applicable.
- SI shall carry out all the electrical work required for powering all the components of the system

- Electrical installation and wiring shall conform to the electrical codes of India.
- SI shall make provisions for providing electricity to the cameras (ANPR, PTZ, and Fixed) via SJB (Surveillance Junction Box), housing the UPS/SMPS power supply, with minimum backup as defined in this RFP,
- For the wired Box cameras, SI shall provision for drawing power through PoE (Power over Ethernet), while PTZ cameras shall be powered through dedicated power cable laid separately along with STP/SFTP cable.
- Registration of electrical connections at all field sites shall be done in the name of Authority.
- SI shall house the electricity meters inside the power cabinet as mentioned in the controller Cabinet section as above.

Earthing and Lightning Proof Measures

1. SI shall comply with the technical specifications taking into account lightning-proof and anti-interference measures for system structure, equipment type selection, equipment earthing, power and signal cable laying. SI shall describe the planned lightning-proof and anti-interference measures in their technical bid.
2. Corresponding lightning arrester shall be erected for the entrance cables of power line, video line, data transmission cables.
3. All interface board and function board, interfaces of equipment shall adopt high speed photoelectric isolation to reduce the damage to integrated circuit CMOS chip due to the surge suppression.
4. Install the earthing devices for the equipment, including lightning earthing, protection earthing and shielded earthing. All earthing shall meet the related industry standards.
5. The earthing cable shall be installed in a secure manner to prevent theft and shall be rust proof. Earthing down lead and the earthing electrode shall be galvanized

Miscellaneous:

1. Authority shall assist in obtaining all necessary go ahead, legal permissions, NOC (No Objection Certificate) from various departments to execute the project. SI shall have to identify and obtain necessary legal / statutory clearances for erecting the poles and installing cameras, for provisioning of the required power, etc. SI shall provide & manage all necessary paper work to pursue permission from respective authorities. No commercial/legal fees (except the RoW charges) shall be applicable to Authority for obtaining the necessary permissions. These shall be provisioned for by the SI in their financial bid.
2. The SI shall provide all material required for mounting of components such as cameras, VaMS and other field equipment. All mounting devices for installation of CCTV cameras to enable pan and tilt capabilities shall be included in the costs of the respective component. The same is also applicable to crossheads and cross arms, mounting brackets, stainless steel bands, screws and other accessories.
3. All the equipment, software and workmanship that form a part of the service are to be under O&M from the SI throughout the contract period.
4. SI shall also get comprehensive insurance from reputed insurance company for the project duration for all the equipment / components installed under this project.
5. SI shall ensure all the equipment’s installed in the outdoor locations are vandal proof and in case the equipment get damaged /stolen for reasons whatsoever, it shall repair/replace the same in the specified time as per SLAs at no extra cost to the Authority. All such costs shall be factored in the comprehensive insurance of field equipment for the duration of the contract.
6. Preventive maintenance shall be carried out once in a quarter along with corrective maintenance and also when calls are placed by Authority or its designated agency.

7. In addition to above, the SI shall be fully responsible for all maintenance activities for the period between installation of equipment and roll-out of the system.
8. During implementation, if observed that any camera / field equipment requires change in the field of view / orientation, it shall be done by SI without any extra cost.
9. In case of request for change in location of field equipment post installation, the same shall be borne by Authority at either a unit rate as per commercials or a mutually agreed cost.

4.17.6 Public Address system

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.

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).

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.

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.

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
9.	Operating conditions	0° to 50°C

4.17.7 Variable Message Signboards

Variable Message Signboard (VaMS) shall be installed at identified strategic locations. The VaMS shall communicate information & guidance about traffic, diversions etc. to the citizens / public on the road. They shall also be used for showing emergency/ disaster related messages as and when required. The SI shall describe in detail the design, operational and physical requirements of the proposed Variable Message Signboards to demonstrate compliance with all the specified requirements in this RFP.

The VaMS unit shall be able to communicate with the Command Control Centre system using GSM Data/ Wi-Fi/ Ethernet/SMS Channel. GSM data channel (GPRS) / Wi-Fi/ Ethernet shall be used to send online messages and SMS channel shall be used to send configuration packets to configure the SIM. Ethernet port shall also be extended to ground level using necessary cables for local troubleshooting. Each unit shall be provided with a unique identification number and shall communicate with the Command Control Centre system.

VaMS shall be managed and operated from the Command Control Centre handled by a server where information in the form of data messages shall be fed in a manner to be displayed on a specific VaMS installed at a particular location or across all locations. The VaMS shall be viewable from a distance of 100m and various angles on the road.

For installing VaM Signboards, the SI shall provide Gantry with spans, as required at various locations (single lane road, double lane road). Spans need to be specified depending on the number of lanes that need to be bridged. SI shall consider additional space for lateral clearance as well as a vertical clearance height as per NHAI (National Highway Authority of India) guidelines.

Functional Specifications:

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

b) VaMS 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 VaMS 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) VaMS 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) VaMS 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 VaMSs.

g) VaMS 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 VaMS.

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 VaMSs 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.

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

	Specifications	Minimum Requirements
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.
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

	Specifications	Minimum Requirements
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 VaMS (Control Messaging Application at Data Center)

The Application System for Controlling Messaging for VaMS shall:

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

4.17.8 Drone based Surveillance

Drones are airborne systems providing advanced surveillance solutions that can be used by law enforcement agencies to monitor situations like large scale crowd gathering, processions, dharnas, Rasta-roko and similar surveillance purposes wherein the incidents like stampede, chaos etc., may happen causing irrevocable aftermath.

Remote-controlled drone could be flown to incident locations and scenes of accident. A high resolution camera is mounted on the drone that can rotate to have a complete 360^0 view of the ground and the data is transmitted to the command control room providing a real time awareness of the situation thus facilitating the authorities to assess and control the situation and prevent any untoward incidents. Preventive measures could be properly assessed and planned in advance in case of any further events.

High resolution photos received from the feeds can be stored as records and can provide valuable evidence for subsequent analysis.

The drone should be low weight and should have a min flight time of 60 min. It should be able to operate in all weather conditions including night time. It should have min 30 min battery backup and should cover min 5 km range.

It should record videos in all the common video formats. There should be provision to take snapshots. It should have PTZ and altitude control functionality and functionality to download maps upon entering the GPS location.

4.17.9 Mobile Surveillance Vehicle

The Mobile Surveillance Vehicle (MSV) is a surveillance vehicle that dramatically increases the surveillance, protection & localized command capabilities as a mobile operational unit. This system could be installed on any suitable vehicle (preferred Innova diesel GX2.5 or similar type), and has a vital "look-up and see" capability to cover a wide area of security operations. The flexible modular architecture of the MSV system enables progressive system growth with connectivity to Command Control Centre. The MSV shall have feature for real-time data link communication, transmitting video and receiving data simultaneously.

1. The MSV shall be a fully customizable vehicle unit with rapid deployment capability within the Kakinada environment and other rugged terrain in all weather conditions. The entire solution is to be made ruggedized to handle vibration and shocks during transportation. The fully mobile van can easily be deployed at any location for surveillance.
2. The specialized vehicle shall have capabilities for data processing, real-time communication and situational analysis. It shall work as a mobile surveillance command center.
3. The vehicle shall have a PTZ camera mounted on top and two fixed box cameras all equipped with Infrared capability to see during low light conditions. The PTZ camera shall be mounted on a retractable hydraulic shaft arrangement.
4. The registration of MSV under the Project shall be in the name of Authority/City Police.
5. The vehicle can be divided into three main sections:
   a. Driver Side
   b. Monitoring Side
   c. Power Compartment
6. Provision for Firefighting equipment in the MSV

The driver side section of the MSV shall house space for one driver and one passenger. The monitoring side of the MSV shall have seating for at least two personnel who shall monitor the cameras (PTZ camera) on on-board screens. The monitoring section shall also have LED screens, laptop etc. All the cameras in the MSV shall have the Video Management Software and Video Analytics software

A portable generator shall be installed in the vehicle to power surveillance equipment. The portable generator shall be of necessary capacity to support equipment's' installed in MSV. A UPS shall also be installed in the MSV of adequate capacity.

MSV operator shall be empowered to monitor, coordinate and relay commands too & fro with the field units and Command Control Centre. The vehicle should also include, a PA system to broadcast for the outside people.

Other supporting components shall include but are not limited to:

1. Observation hatch on the roof
2. Siren with integrated PA system
3. Flame Proof - water proof cabins
4. Search lights
5. Mobile office Seating arrangement
6. LCD screen
7. Power Generator/ UPS for uninterrupted power supply
8. Air-conditioning
9. First-aid Box
10. Umbrellas, Torches etc.

4.18 Command and Control Center (CCC) – Kakinada City Surveillance

State-of-the art Command Control Centre is required to be established as part of the Kakinada Surveillance solution. The proposed CCC shall handle feeds from the cameras and display them on the Video wall and provide necessary interface for integrating with other applications like Dial 100 and response mechanism as required by the Authority, it shall present a Common Operating Picture (COP) of the real time events in the area of purview.

4.18.1 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.

4.18.2 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

Functions of the Command Control Centre shall include but not limited to the following:

1. Video Surveillance
2. Video Investigations
3. Emergency Response activities
4. Video data storage & retrieval

The Command Control Center shall be working in a fully automated environment for optimized monitoring, regulation and enforcement of traffic with various law enforcement services. Various applications/ modules like ANPR, RLVD, FRS specified in this RFP shall be integrated into one functional system and shall be accessible by the operators and concerned agencies with necessary login credentials. The operators/end users shall be able to access master data like Vahan and Sarathi databases (that are available with the agencies and that can be integrated as and when available). The integration with such systems will be in the scope of the SI.

Location for Command Control Center shall be provided by the Authority. Responsibilities of the SI shall include site preparation activities as mentioned in this RFP. The SI shall ensure that the Command Control Center shall control and integrate systems in a seamless manner.

i. The Command Control Center shall provide a comprehensive system for planning, optimizing resources and response. The system shall thus be an "end to end" solution for safeguarding and securing people and assets for the purpose of preserving operational continuity. The minimum technical specification for the equipment required at the Command Control Center is listed in this RFP.

ii. The SI shall be required to undertake detailed assessment of the requirements at the command control center and prepare a plan to implement the Command Control Center and commission required IT and non-IT infrastructure and also carry out the civil/ electrical work as required.

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

iv. The video feed from the surveillance cameras shall be received at the Command Control Center where a video wall shall be installed for viewing.

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

4.8.3 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.
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.

#	Functions	Minimum Specifications
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 Kakinada (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.

#	Functions	Minimum Specifications
27.		Provide User-defined forms as well as Standard Incident Command Forms for incident management.
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.

#	Functions	Minimum Specifications
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.
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.

#	Functions	Minimum Specifications
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.
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.

#	Functions	Minimum Specifications
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.
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

#	Functions	Minimum Specifications
		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.
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 multidimensional 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

4.18.4 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.

4.18.5 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 Kakinada 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.

4.18.6 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
1.	Screen Size	55” or higher
2.	Resolution	Full high definition (1080p) 16:9 Widescreen
3.	Contrast ratio	5000:1
4.	Brightness	350 nit
5.	Viewing angle	178 degree/178 degree (H/V)
6.	Response time	8ms
7.	Input	HDMI
8.	Control	On Screen Display (OSD) IR remote control
9.	Operations	24 x 7 basis

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	DVI/HDMI/USB/ LAN/ VGA/SATA port
12	Accessories	104 key Keyboard and Optical USB mouse
13	USB Ports	Minimum 4 USB Ports
14	Redundancy support	Power Supply, HDD, LAN port & Controller
15	Scalability	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

#	Parameter	Minimum Specifications
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	Display & Scaling	Display multiple sources anywhere on display up to any size
2	Input Management	All input sources can be displayed on the video wall in freely resizable and movable windows
3	Scenarios management	Save and load desktop layouts from local or remote machines
4	Layout Management	Support all layout from input sources, Internet Explorer, desktop and remote desktop application
5	Multi View Option	Multiple view of portions or regions of Desktop, multiple application can view from single desktop
6	Other features	SMTP support
7		Remote Control over LAN
8		Alarm management
9		Remote management
10		Multiple concurrent client
11		KVM support
12	Cube Management	Cube Health Monitoring
13		Pop-Up Alert Service
14		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.

#	Parameter	Minimum Specifications
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
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

#	Parameter	Minimum Specifications
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 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

Sl No	Item	Minimum Specifications
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

Sl No	Item	Minimum Specifications
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
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 preloaded (at the facility of OEM or any other location) before shipment to Authority offices/locations.

7. Laptop

Sl No	Item	Minimum Specifications
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.

Sl No	Item	Minimum Specifications
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
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). This software shall be pre-loaded (at the facility of OEM or any other location) before shipment to Authority offices/locations.

8. Network Color 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

9. 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

#	Parameter	Minimum Specifications
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

10. 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

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

10. Radio Handset

Bidder shall visit Kakinada Police Dept. and the Radio Handset should be similar to the one used by the Police Dept.

#	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-synchronization, Keystone Correction

4.18.7 Dial 100 Control Room

A Dial 100 Control Room shall be established as part of the command control center in the Kakinada. A Dial 100 based police control room would empower people to connect to police and get police assistance anytime, anywhere at very short “response time”.

The objective of the Dial 100 Police Control Room is to receive and respond immediately to emergency calls made by the public seeking police assistance by directing the patrolling police vehicles available for the purpose. The center will be equipped with latest technological tools like GIS MAP, CAD (Computer aided dispatch) and GPS enabled PCR VANs to attend to handle public distress calls for services.

The dial 100 control room shall be provided with one PRI line inline hunting-single telephone number (100) to a group of 30 lines. Number of incoming and outgoing calls can be defined as per requirement for each Kakinada. The Dial 100 control system aims to ensure that:

i. Calls can be made to 100 from any phone whether landline or mobile.
ii. System has multiple caller interface and is capable of receiving 30 calls at a single instance.
iii. Caller’s name and address is automatically visible saving precious time.
iv. Exact location of the place of incident and nearest available police vehicle identified on GIS map which saves time.
v. Status of response by police vehicle can be monitored by control room.
vi. Information received and police actions taken are automatically logged into the system generating a fool proof database of events.
vii. The system should have facilities such as cell ID, Observed Time Difference of Arrival (OTDOA) and assisted GPS to acquire and push accurate location information for both wireless and wireline phone to emergency.

All communications in the call centre shall be recorded for future reference. 50 TB storage capacity shall be allocated for recording voice communication through telephone line and radio gateway. The stored communication shall be available for hearing at any future point of time. The dial 100 control room shall be equipped with IT and Non-IT hardware and software.

a) Functional Requirements

1. The basic requirements of Police for setting up Dial 100 Control Room include but not limited to:
   a. Establishing a quick and efficient emergency response system
   b. Dispatch vehicles rapidly to required location
   c. Automation of Call-taking & Dispatching
2. The Computer aided dispatch (CAD) software platform integrates various modules:
   a. CAD framework
   b. Call Reception System
   c. Call Recording and Logging
   d. GIS (Geographical Information System)
   e. AVLS (Automatic Vehicle Location System)
   f. Responder Systems (Mobile Data Terminals)
   g. Incident Reporting System
   h. Video Interface (CCTV Video Integration to GIS)
   i. Converged Communication Platforms [PSTN, Wireless (Cell Phone), SMS, e-mail]

The Integrated Software Platform supports all features required for efficiently handling all stages of a call made in emergency situation.

b) Operational Requirements

1. Dial 100 control room shall be equipped with EPABX comprising of 1 PRI line inline hunting-single telephone number (100) to a group of 30 lines in each Kakinada.
2. The Control room shall have seating capacity of minimum of 15 operators
3. Citizen can dial 100 for any complaints related with police. The system shall have capability to display name, address and find the geographical position of the caller at the time of receiving call in call center.
4. All phone calls shall be recorded for future references. The phone calls of last at least 90 days shall be stored in SAN Storage.
5. Dial 100 operators shall be able to receive call, Dispatch calls, use GIS maps and can send the alerts to the nearby free Patrolling vehicles on their MDT and also inform the nearest Police Station about the event.
6. Dial 100 operator shall be able to view the nearest Fire Station, Hospital, Blood Bank for providing additional assistance at the site of incident.
7. Dial 100 operator shall also be able to use police radio network for emergency handling and for communication with PCR Vans etc.
8. A web based incident analytic software shall be made available that will help the Police to do detailed analysis and analytics so that the response can be made proactive and also the effectiveness of the service improved.
9. After the Call has been logged in by the call taker, the Dial 100 System shall send a SMS to the Caller stating the CFS/Tracking Number along with a password as acknowledgement to the call made to the control room. The caller can use this number on department website to access the event progress details such as Action Taken Reports (ATR), file attachments, remarks, or other information's as per the prevailing departmental policy for data sharing.
10. The analytics should have Social Media Analytics as one of the components. The Kakinada city police and public functionalities need to be in touch with and being accessible to the general citizens especially the youth, senior citizens and media etc. especially through social media. The analytics would leverage highly unstructured social media data in real time by using streaming social media analytics to identify rumors, potential threats and evolving events, find evidence through photos or track down witnesses. The analytics would also acquire location and tactical information of victims or criminals from information posted on Twitter, Facebook or other social media

4.18.8 Emergency Call Box

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.

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, Colour 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

4.18.9 Forensic Investigation Room:

The Command Control Centre will also have a room identified for IT Analytics and Forensic Experts where they will analyze the incriminating video clips and certify its integrity & chain of custody. The analysis would primarily relate with Video Analytics. The forensic Investigation room shall be equipped with one video wall, five workstations, IP telephone and at least five operators. Each Kakinada shall have its own forensic investigation room. The operators in the forensic room shall have access to live as well as stored video.

The operators would be able to run video analytics software on video digital feed being received from camera selected for the purpose. The forensic operators shall have access to all recorded voice communications of Dial 100 control room.

The analysis in C4 would be graphical user interface for search, replay and to simultaneously search and replay recorded telephone systems, GPS data on GIS maps, conventional and digital radio channels as well as trunked radio communications. All communications regarding a specific incident should be able to be replayed together in the sequence in which the communications occurred on a synchronized timeline. System should support following Analytics:

- Unidentified object detection
- Intruder detection
- Camera tampering detection
- Virtual Fence / Tress Passing / Tripwire
- People / Mass movement
- Wrong direction monitoring

SI should provide option to run these analytics at edge level so that bandwidth can be saved or server based analytics can also be offered in case of proposed camera do not have capabilities of running analytics on the edge.

Video Analytics system shall provide mechanism to allow alerts to be raised in a customized manner for C4, Police officials and automatic decision support system. System shall be capable of avoiding generation of false alarms

The VMS shall allow access of the video feeds on Tablets/iPads/select devices on user request. Such an access shall be based on MAC Address authentication over SSL (Secure Socket Layer) and/or by creating a VPN (Virtual Private Network). In addition, the VMS should be able to stream feeds from authorized Tablets/iPads/mobiles/select devices on the Video Wall.

The C4 should have the facility of integrating Police (100), Fire (101) and Health (102/108) Services. Coordination with these agencies is critical. The integration shall be for recording of all the data types of the above services as well as for real time transactions and response. The operators within C4 (Video Surveillance room and dial 100 room) shall make prompt and accurate decisions as per requirement of the incident, using the available technology. The center should also be able to group locations and connect surveillance systems in order to respond quickly to any emergency.

The suite of software modules would be required to be scaled up to support any number of cameras, control rooms and client operators and would have multiple redundancy and security level options.

Forensic Investigation Room – Operational Requirements

1. Forensic Investigation room shall be equipped with one video wall, four workstations, IP telephone and at least five operators in the Room.
2. The forensic investigation room shall have seating capacity for min. 5 operators.
3. The forensic operators shall have facility to see live as well as playback videos of any camera. They shall keep a special watch on few selected cameras.
4. The video analytics software shall run on selected camera feeds to be further investigated by forensic operators.
5. The forensic operators shall be equipped with software for :
   - examination of authentication of uploaded photos and videos
   - repair and recover videos
   - match photographs
   - provide forensic video enhancement of video evidence for identifying suspects,
   - provide recorded and archived media to authorized persons
   - transfer the evidence into a format that can be used for legal purposes etc.
   - Post analysis of video provided through secondary source through various attributes like identified object, size, color etc.
     1. The forensic operators shall also have access to recorded voice communications of dial 100 control room and radio gateway.
     2. Forensic Analyst/Operator may have following roles and responsibilities:
        I. Examine, enhance and authenticate digital and analogue CCTV video evidence for both criminal and civil litigation
        II. Assist the police in respect of preparation of evidence for legal and judicial purpose in court.
        III. Providing recorded and archived media to authorized persons.
        IV. Transfer the evidence into a format that can be used for legal purposes
        V. Provide Forensic video enhancement of video evidence for identifying suspects.
        VI. Attending and examining scenes of crimes
        VII. Repair and recovery of evidence

4.18.10 Application Environment:

a. Video Management System

Video Management System (VMS) shall bring together physical security infrastructure and operations and shall use the IP network as the platform for managing the entire surveillance system. End users shall have rapid access to relevant information in digital format for quick analysis.

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

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

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

1. The VMS shall support a flexible rule-based system driven by schedules and events.
2. The 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.
3. The VMS shall support IP cameras of different makes.
4. All the offered VMS and cameras shall have ONVIF compliance.
5. The VMS shall be enabled for any standard storage technologies and video wall system integration.
6. The VMS shall be enabled for integration with any external Video Analytics Systems
7. The VMS shall be capable of being deployed in a virtualized environment without loss of any functionality.
8. The VMS server shall be deployed in a clustered server environment for high availability and failover.
9. 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 in 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.
10. The VMS shall have an administrator interface to set system parameters, manage codecs, manage permissions and manage storage.
11. The VMS day to day control of cameras and monitoring on client workstations shall be controlled through the administrator interface.
12. Whilst live control and monitoring is the primary activity of the Operator workstations, video replay shall also be accommodated on the GUI for general review and also for pre and post alarm recording display.
13. The solution design for the VMS shall provide flexible video signal compression, display, storage and retrieval.
14. All CCTV camera video signal inputs in digital format to the system shall be provided to command control Center, and the transmission medium used shall best suit the relative camera deployments and access to the CCTV Network.
15. The VMS shall be capable of transferring recorded images to recordable media (such as CD/DVD and/or DAT tapes) in tamper evident and auditable form. All standard formats shall be supported including, but not limited to:
    a. AVI files
    b. Motion- Joint Photographic Experts Group (M-JPEG)
    c. Moving Picture Expert Group-4 (MPEG-4)
16. All the streams shall be available in real-time (expecting the network latency) and at full resolution. Resolution and other related parameters shall be configurable by the administrator in order to provide for network constraints.
17. The VMS shall support field sensor settings. Each channel configured in the VMS shall have an individual setup for the following minimum settings, the specific settings shall be determined according to the encoding device:
    a. Brightness
    b. Contrast
    c. Color
    d. Sharpness
    e. Saturation
    f. Hue
    g. White balance
18. The VMS shall support the following minimum 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)

19. 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.
20. The VMS shall support bookmarking the videos. Thus, allowing the users to mark incidents on live and/or playback video streams.
21. The VMS shall be capable of intrusion detection*:* Detection of moving objects in selected areas covered by the camera (those that are specified as restricted areas like those before some major events, etc.). Avoid false alarms due to wildlife or other moving objects (e.g., tree leaves).
22. The VMS shall be capable of tracing of a specific person or object in multi-camera videos*:* Track a specific person or object across several surveillances (e.g., to trace and identify criminals and/or anti-social elements).
23. The VMS shall be capable of counting of people and detection of abnormal crowd behaviour*:* Detection of people flow and counting of people in selected areas. To identify abnormal crowd behaviour and raise alarms to avoid untoward incidences in public places, and maintaining law & order.
24. The VMS shall be capable of summarize videos and create a content summary of the captured video depicting relevant movements or objects of interest. This would on *off-line* as well as *online* videos captured by the camera. For example, an hour-long surveillance video could be shortened by considering only the frames that depict major movements in the video.
25. 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.
26. VMS shall support automatic failover for recording.
27. VMS shall support manual failover for maintenance purpose.
28. VMS shall support access and view of cameras and views on a smartphone or a tablet.
29. VMS shall support integration with the ANPR application.
30. VMS shall support integration with other online and offline video analytic applications.

i. VMS Core Components

1. *CCTV Camera Management* – Shall enables management of cameras associated with the VMS.
2. *Video recording, retrieval and archiving* – Shall manage live camera viewing, recording of live feeds for future review, search and retrieval of recorded feeds and archiving of recorded video feeds for optimum utilization of resources.
3. *Video Analytics (VA) alert management – Shall e*nable defining of rules for handling of alerts using the VA handling of events as per the defined rules.
4. *MIS and Reporting – Shall p*rovide users with business analytics reporting and tools to organize evaluate and efficiently perform day to day operations.
5. *Security and Roles – Shall m*anage role definitions for internal as well as external access.

ii. VMS General

1. The VMS shall be Codec and IP camera agnostic such that it can support devices that are not supplied by the manufacturer/developer of the VMS software and Codec hardware.
2. Each camera shall be identified by giving it a minimum thirty-two (32) character long, alphanumeric unique id followed by text description field.

3. When viewed on the GIS map, the text description of each camera shall be capable of being positioned anywhere on the monitor screen, on a camera by camera basis, shall afford options for size variations, and display with a flexible solid, semi-transparent or transparent background.
4. The VMS shall support tamper detection for all cameras to warn of accidental or deliberate acts that disable the surveillance capability.
5. For alarm interfacing requirements, the VMS shall allow the selection of minimum five (5) cameras per single alarm source. The designated primary camera shall be automatically displayed as a full-screen image on the main GUI CCTV screen. The VMS shall also, on alarm, present associated pre/post event video allowing the Operator to assess the alarm cause. Other associated cameras, when called up, shall be displayed as split-screen images on the other monitor of the operator workstation.
6. Playback of any alarm related video, (including pre and post alarm video) shall start at the beginning or indexed part alarm sequence.
7. Video management software shall incorporate online video analytics on live video images. It shall include the following video analytics detection tools:
   a. Presence detection for moving and stopped vehicles
   b. Directional sensitive presence detection
   c. Congestion Detection
   d. Loitering detection
   e. Improper Parking
   f. Camera Tampering
   g. Abandoned objects detection
   h. Gun-shot detection
8. Off- Line Video Analytics should allow for quick retrieval of video footage to metadata stored with each image. System should provide results within few seconds, system should support for below listed the user's query.
   a. System should allow to specify the following search criteria:
      i. Motion in the zone, user-defined with any polyline
      ii. Detection of crossing a virtual line in a user-defined direction
      iii. Loitering of an object in an area
      iv. Simultaneous presence of a few objects in an area
      v. Motion from one area to another.
   b. System should support to apply below listed filters to search results:
      i. Object size
      ii. Object color
      iii. Direction of object motion
      iv. Speed of the moving object
   c. Defined area entry/appearance and zone exit/disappearance
9. Video clips of specific events via the VA or by the operator action shall be capable of being separately stored and offloaded by operator with appropriate permissions on to recordable media such as CD or Write Once Read Many (WORM) together with any associated meta-data for subsequent independent playback.
10. The system shall provide the capability to select duration and resolution of storage by camera, time and activity event and user request. Frequency/trigger of transfer shall be configurable by user.
11. The system shall provide the capability to digitally sign recorded video.
12. **Live video viewing:** The system shall allow the viewing of live video from any camera on the system at the highest rate of resolution and frame rate that the camera shall support on any workstation on the network.

13. **Recorded video viewing:** The system shall allow the viewing of recorded video from any camera on the system at whatever rate the camera was recorded.
14. **Storage of video:** The system shall store online thirty (30) days of video for all cameras. Balance 60 days will be on low cost secondary storage /tape library
15. The system shall provide the capability to manage the video storage to allow selective deletions, backups, and auto aging.
16. VMS shall have an extensive reporting capability with ability for administrator to define reports in a user friendly manner. The pre-existing reports shall include, but not limited to, the following:
    a. Reports on alerts received by type, date and time, location
    b. Reports on system errors and messages
    c. Reports on master data setup including cameras, decoders, locations
    d. Reports on cameras health check
    e. Reports on audit trails such as user actions
    f. Reports on system health including storage availability, server performance, recordings

iii. VMS GUI Capabilities

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

iv. VMS Map Functionality

1. The system shall support a mode of operation whereby a map of all or part of the map (at operator request) is displayed on a separate or same screen and that status information can be provided via an icon, and access to any cameras shall be accessible by means of an icon on that screen.
2. These Maps shall be defined so that an operator may make a selection from the same source of mapping that is available to the other systems within the command control center, displaying whichever Map or section the operator needs, and it shall be displayed within one (1) second.

v. VMS Configuration

1. The VMS shall include a configuration facility to provide system administrators with a single interface utility to configure all VMS operating parameters.

2. The configuration tool shall be capable of supporting multiple concurrent users of the system, providing the ability to automatically update. It shall also allow the codec and camera configurations to be imported and exported in excel format.

3. The import/export tool shall be as sophisticated as necessary to support the following:
   a. Log every action so an audit or report can be completed
   b. Only update and log configurations where there is a difference between the system configuration and the new configuration file to be loaded
   c. The import configuration file can contain any amount of data
   d. Ability to run an update on the fly - i.e. no or minimal downtime to the system
   e. Not require a reset or restart after any upgrades
   f. Definable update times
4. The VMS configuration tool shall define:
   a. Cameras (whether via codec units or directly connected IP cameras) and text based names
   b. Camera Groups
   c. User Groups
   d. Monitors
   e. Codec parameters
   f. Alarms
   g. Workstations
   h. storage
5. The configuration utility shall allow the system administrator to:
   a. Install new devices
   b. Configure all aspects of existing devices
   c. Configure and set up users/user groups and their rights/permissions/priorities
   d. To define multiple camera groups
   e. Each group to be defined for combinations of viewing and control rights
   f. Individual Operators to be assigned multiple groups
   g. Each group to be allocated to multiple Operators
   h. Each camera may be in multiple groups
   i. To program macros for individual and group camera characteristics
   j. Program camera/monitor selection and configuration of the video wall(s) in response to an incoming alarm
   k. Designate workstation destination for picture presentation in response to alarm initiation
6. User permissions/privileges, to be allocated, shall extend from full administrator rights down to basic operation of the system, and shall include the ability to designate workstations to an operator, and to designate one or more camera groups to an operator for viewing and/or control.

7. The configuration utility shall store all changes to the system, including but not limited to:
   a. User log-ins
   b. User log-offs
   c. Human interface device inputs (key strokes)
   d. External alarm commands
   e. Error messages
8. A copy of the system configuration shall be stored external to the system to allow system restoration in case of hardware failure. External would mean another site, to be agreed with Authority during detail design.

vi. VMS User Hierarchy

1. The System Integrator shall request a detailed User Prioritization List (UPL) from the Authority during the project.
2. The UPL shall enable the programming of the CCTV management system with the agreed user prioritization.
3. Over and above user priority, users shall be enabled for the following in varying combinations:
   a. Image viewing
   b. Image recording
   c. PTZ control
4. In addition, the control location shall be prioritized as such that the command control Center has full control of all functions and priority one (1) override over all other locations.
5. Within the hierarchy, each user's log-on password shall not only allow access to varying levels of system functionalities, but shall also provide for a relative priority between users of equal access rights. In this manner, operators in the above groups shall be individually allocated a priority level that allows or denies access to the functions when in conflict with another operator of lower or higher priority level.
6. These priority levels and the features they contain shall be discussed and defined with the system administrator. The SI shall allow time to carry out this exercise together with the relevant configuration of groups, sub-groups, permissions and priorities.

vii. VMS Recording Requirements

1. All images shall be recorded centrally as a background process at configurable parameters.
2. It shall not be possible to interrupt, stop, delay or interfere with the recording streams in any way, without the appropriate user rights.
3. The CCTV recording system shall enable pre and post event (PPE) recording, presentation and storage, initiated automatically in response to system alarm sources received by the VMS.
4. The PPE recording clips shall be provided by the VMS and retrieved from the central video archive on the buffer storage system. This PPE stream shall be totally independent of the background recording stream provided to the central video archive such that central video archive recording, as programmed, continues under all circumstances.
5. The information stored shall be full real-time and full resolution from each incoming camera channel. In the absence of a trigger from a manual input or from a programmed alarm source, the PPE video recording shall be written to buffer storage on a FIFO basis.
6. PPE periods initiated by a single alarm occurrence shall be configurable via the VMS as follows:
   a. Pre – 0 to 30 seconds
   b. Post – 30 to 300 seconds
   c. Shall be variable for each camera according to each individual alarm and the alarm type
7. In the event of a trigger, the VMS shall ensure that the programmed sections of pre

and post event video are immediately presented to the Operator to complement the alarm display and simultaneously saved as an identified indexed video clip, complete with time/date stamp, in a reserved and protected area of the storage system. Such PPE recording shall then be capable of later retrieval via search criteria.

8. Once tagged and saved, the PPE video clip shall NOT be overwritten except by an operator with the required permissions i.e. it is excluded from the normal FIFO regime of the bulk storage system. Recording shall also be initiated on-demand by manual triggers from system operators e.g. keyboard key-stoke.
9. The VMS shall support the following recording modes:
   a. Total recording – the VMS shall constantly record the video input. The VMS shall allow for continuous recording of all video inputs
   b. Event based recording – the VMS shall record the video input only in case an event has occurred
10. VMS shall support the following triggers to initiate a recording
    a. Scheduler – the recorder will record the video inputs based on a specified scheduler
       i. The VMS shall allow recording based on a time schedule for all or some of the video channels
       ii. The VMS shall allow for multiple recording periods per day, per channel
       iii. The VMS shall have the option to set any available trigger in the system (VMD, TTL and/or API) to trigger the channel
       iv. The VMS shall have the option for individual channel setup of pre/post-alarm recording for defined interval (e.g. up to 10 minutes pre-alarm and 30 min post-alarm recording)
       v. The VMS shall have the ability to enable/disable triggers through a daily time schedule
    b. Manual – the user shall be able to initiate a manual recording upon request.
       i. The VMS shall work in conjunction to the any previous alarm operations
    c. The VMS shall allow API Triggers
    d. All trigger information shall be stored with the video information in the VMS data set and shall be made available for video search

viii. Manual or on demand recording

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

ix. VMS review system

1. The VMS recording and replay management systems shall support the following features and operations:
   a. Play back shall not interfere with recording in any way
   b. Support either analogue cameras connected via Codecs or IP-cameras directly connected to the network
   c. Stream live images through the network using IP Multi-cast techniques
   d. Stream images from the Codec to the attached storage system
   e. Store the recording stream from all cameras simultaneously with no degradation to any individual camera recorded image stream unless the system is configured by administrator to allow for change in quality
   f. Deliver live video to VMS workstation within a period of one second from manual call up

g. Deliver live video to VMS workstation within a period of three seconds from automatic alarm receipt on alarm interface

h. Storage of each camera's images at a rate and resolution as defined in the Codec or IP camera configuration. The system VMS programming shall automatically vary these rates in response to time profiles, alarm inputs

i. Support multiple, configurable recording time schedules per camera. Each schedule shall support different recording parameters and automatically implement against the configured time schedule e.g. operational and non-operational hours shall be scheduled with different recording parameters on designated cameras

j. Support streaming of recorded files using IP Unicast directly to hardware decoders for display on analogue monitors or software decoder when/if required

k. Playback multiple, synchronized recorded streams at differing speeds and frame rates

l. Record and playback a video stream simultaneously at differing speeds and frame rates

m. Time stamping of every recorded video field based upon Network Time Protocol (NTP) time

n. Selectable on-screen-display of time and camera title during playback

o. Security file lock to prevent specific recorded files from being overwritten regardless of their date and time, in addition to those records stored as PPE clips. The duration and policy for retention of such videos would be same as that of the PPE clips

p. Configurable granularity of video files

q. Generate alarm when storage medium has fallen below a user selectable threshold

r. Stored video files can be "down-loaded" to directly CD ROM and/or DVD or WORM for replay using the VMS video replay application, and shall incorporate proof of authenticity Kakinada

s. Download video records in common (e.g. AVI) file format for remote, cursory review and assessment prior to generating tamper-evident auditable copies

x. VMS alarm handling

1. The video alarm handling shall provide the following facilities for the handling and management of video images generated by alarms associated with other systems integrated with the VMS.
2. Whilst the pre and post alarm requirement has been included (up to thirty (30) seconds pre alarm, three hundred (300) seconds post alarm per camera at fifteen (15) FPS) the VMS shall display and manage the pre and post alarm information as follows for a maximum of two hundred (200) alarms per day:

   a. The pre and post alarm video clip shall be displayed full screen, in real-time and shall continuously play the 'loop' until the operator accepts the initial alarm activation or clears down the event

   b. The pre and post alarm shall be displayed on a dedicated monitor

   c. Each monitoring station shall be able to display simultaneous alarms

   d. The 'video clip' associated with the alarm shall be tagged with date and time etc. and stored in a dedicated location for retrieval at a later date

   e. Alarm archived video shall be readily available for one month but accessible for six months

   f. The VMS shall accommodate at least 100 simultaneously alarm activating CCTV cameras

g. All alarm based images shall be displayed

3. The VMS shall have the capability to automatically display a primary camera, plus minimum of four additional cameras associated with each alarm based on either camera location with respect to the alarm, or a programmed set of parameters defining the associated cameras.
4. The VMS shall also accommodate operator-initiated recording of a given camera. The operator-initiated recording shall:
   a. Accommodate up to a total of atleast 50 cameras simultaneously (all operators)
   b. Record the selected camera/s for an administrator configured number of hours or until stopped, whichever is the sooner

xi. VMS Integration requirements

1. VMS shall be integrated within a consolidated GUI that would include other command control Center systems as well. All events, activations and alarms that occur with the VMS and its sub systems will interact seamlessly between the command and control center sub systems as required
2. Either the OPC or the SDK shall manage the interface between the VMS, GUI and the other Kakinada Management systems as required.
3. The OPC or SDK shall allow the operator workstations to control the VMS irrespective of the vender chosen by duplicating all control functionality of the VMS used for normal day-to-day activities.
4. Alarm linking between VMS sub-systems shall be done at VMS sub-system level to, for example, call up relevant pictures to screens and move PTZ units to pre-set positions in response to alarm and activate video recordings, modifying recording parameters as necessary.
5. All OPC software shall be fully compliant with the OPC specification as set down by the OPC foundation. Any software or products which are not compliant shall be highlighted in the Technical Proposal return. The SI shall indicate in the technical proposal return how the OPC interface shall be implemented.
6. If an OPC interface cannot be provided, an alternative solution shall be provided for this data using a standard open protocol and confirmation as to how this shall be implemented shall be provided in the technical proposal return.
7. If an SDK solution is provided the system shall allow reconfiguration by (Kakinada) and end users without recourse to special languages. A system SDKs shall be supplied with all required supporting software to allow the integration of the system with new devices and systems.

xii. VMS System Size

The VMS shall enable handling of 100 cameras, on day one, as well as future scalability as may be required.

a. Video Analytics

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

Analytics software shall bring significant benefit to review the incidences and look for suspicious activity in both live video feeds and recorded footages.

Minimum video analytics that shall be offered on identified cameras are:

1 Presence detection for moving and stopped vehicles
2 Directional sensitive presence detection
3 Congestion Detection
4 Loitering detection
5 Improper Parking
6 Camera Tampering
7 Abandoned objects detection
8 Gun-shot Detection
9 Unattended object
10 Object Classification
11 Tripwire/Intrusion

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

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

Solution shall be so designed to have Automated PTZ camera control for zooming in on analytics requirements specified herein

4.18.11 Automatic Number Plate Recognition

SI shall provide Automatic Number Plate Recognition (ANPR) solution at the identified locations. SI shall describe in detail, the design, operational and physical requirements of the proposed ANPR system, to demonstrate compliance with all the specified requirements in this RFP.

ANPR cameras shall provide the feed to the command control center, where the ANPR server shall be located. The ANPR server shall process the image using OCR software for getting the registration number of the vehicle with highest possible accuracy. The system shall be able to detect, normalize and enhance the image of the number plate for detection of alpha numerical characters. System shall be able to identify stolen/ suspected vehicles by cross checking the numbers with vehicle database. ANPR software shall be integrated with video management system.

The ANPR system shall provide a user interface with live view of vehicle entry point 24x7, event notification, image captured, number detection and recognition, event reports customized report generation etc.

The analysis of the image captured shall be done in real time. The database so created from the images captured & analysis shall store the following:

1. Details of vehicle
2. Number and time of entries and exits
3. License plate numbers
4. Validation/Analysis results etc.

4.18.12 Red Light Violation Detection (RLVD) system

Red Light Violation Detection (RLVD) system is a system for capturing details of vehicles that have crossed the stop line at the junction while the traffic light is red. System shall be able to automatically detect red light through evidence camera units and other equipment. The information so captured shall be used to issue challans to the violators.

The SI shall describe in detail, the design, operational and physical requirements of the proposed Red Light Violation Detection system, to demonstrate compliance with all the specified requirements mentioned in this RFP.

RLVD solution shall have an overview camera to capture the zoomed out picture of the entire area when there is a red light violation. Light sensors shall be placed to detect the change in traffic light. Once the traffic light has turned red, the sensors shall activate the camera to capture images of the vehicles that jumped the traffic light.

RLVD system, in case of an offence detected, shall capture details such as site name, location details, lane number, date & time, registration number of car and type of offence on the image itself. The system shall also be able to generate number of reports for analysis such as the traffic light with maximum offenders, peak time of traffic offence and other reports in discussion and as per the customization requirement of the Authority.

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.

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

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.

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.

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.

#	Parameter
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

#	Parameter
	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, Registration 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).

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 be 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

4.18.13 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 Police Stations.

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 as mentioned in Annexure II of the RFP document.

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

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 197945:2005(E)	This standard includes capture and storage specifications of face images for human visual inspection and verification of the individuals in Indian e-Governance applications. It specifies a format to store face image data within a biometric data record compliant to the Common Biometric Exchange Formats Framework (CBEFF), given in ISO 19785-1. It also includes best practices recommended for implementation of the specifications in different categories of e-Governance applications. The scope of this standard includes: ➢ Characteristics of Face Image capturing device ➢ Specifications of Digital Face Image & Face Photograph Specifications intended only for human visual inspection and verification ➢ Scene requirements of the face images, keeping in view a future possibility of computer based face recognition ➢ Face Record Format for storing, archiving, and transmitting the information of face image within a CBEFF header data structure for the purpose of interoperability and usage in future for computer based face recognition.

4.18.14 System Integration

The SI shall ensure seamless integration of Kakinada City Surveillance system with an external Geographical Information System (GIS). The GIS console shall allow operators to get an overview of the entire system and access to all system components. GIS shall enable dynamic view of the location and status of resources and objects/sensors. System shall enable authorized user to open a new incident and associate the incident with its geographic location automatically, via the GIS display.

The proposed Kakinada City Surveillance System shall also provision for seamless integration with other government datasets like Vaahan, Sarathi, Dial 100, e-challan etc. as and when they are available from respective agencies. The system shall be capable of providing evidence support for ANPR, RLVD events and integral with e-challan system if required.

4.18.15 Surveillance Equipment

The project includes surveillance of about across Kakinada 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 Kakinada 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 Kakinada 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 Kakinada 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, Kakinada

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 Kakinada 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 Kakinada 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.

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 and Control Center Requirements

- ✓ 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 e-Challan, 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 & Kakinada 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. o 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.

4.18.16 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, 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. 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

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
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

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
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 a 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.

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
12.	Auto adjustment + Remote Control of Image settings	Colour, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, Gain Control, , Electronic Image Stabilization

#	Parameters	Minimum Specifications or better
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

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.

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

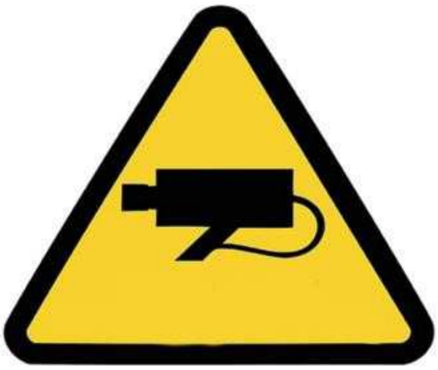
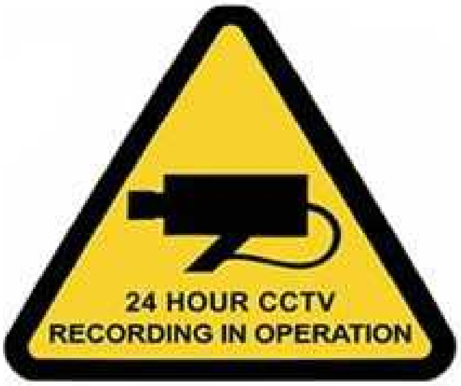
Industrial Grade outdoor PoE switches

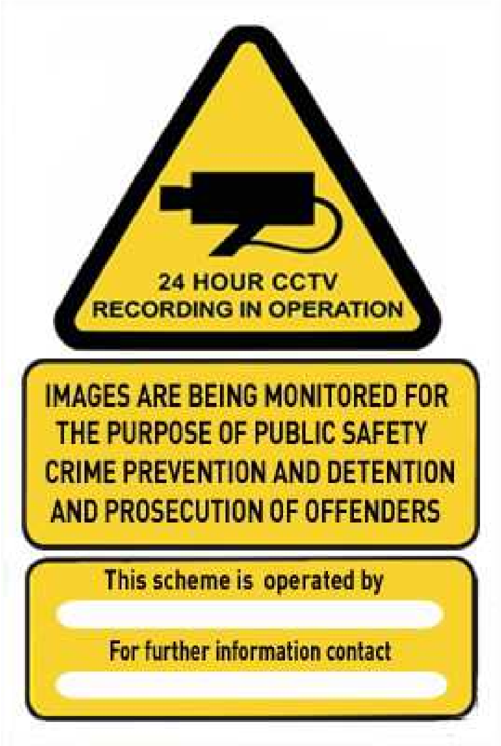
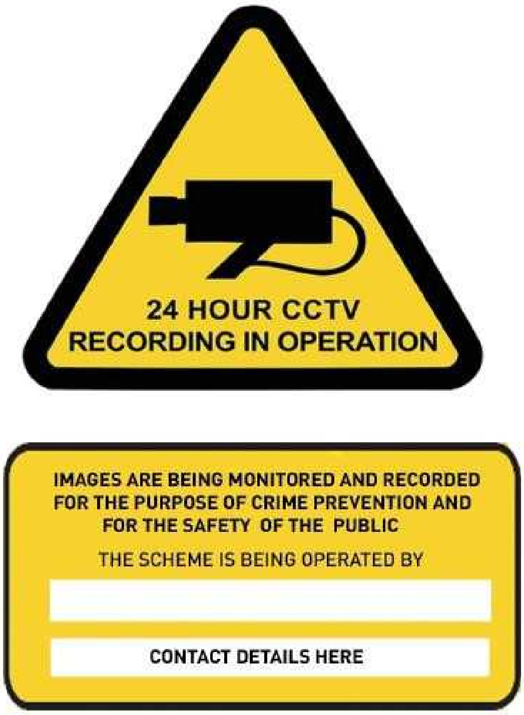
#	Parameter	Minimum Specifications
1.	Type	Managed Outdoor switch
2.	Ports	• Minimum 4 10/100 TX PoE • May require higher port density at some locations, depending upon site conditions • May require fiber ports at some locations, depending upon site conditions/distances.
3.	PoE Standard	IEEE 802.3af 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

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)

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.
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

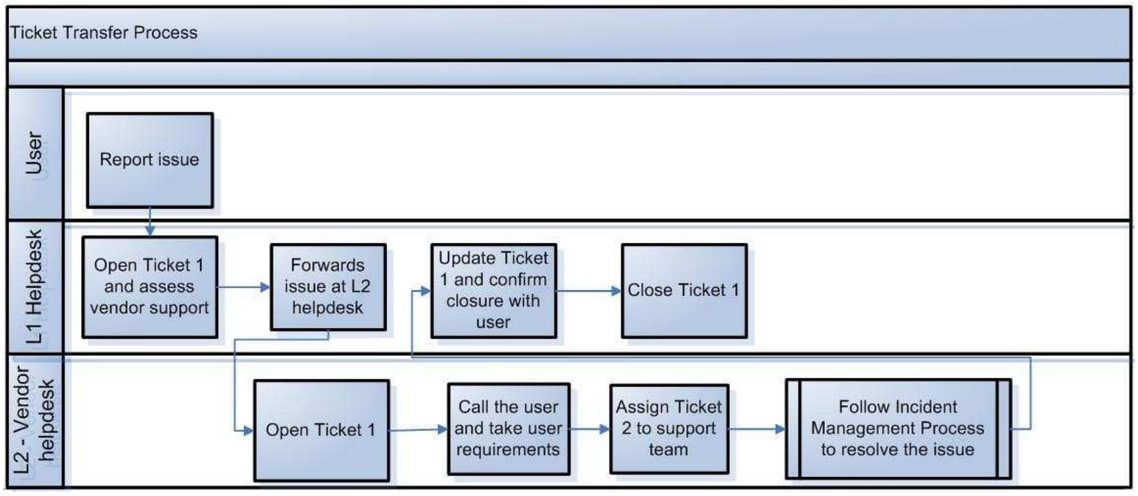
Type	Sign Design	Remarks
C	 24 HOUR CCTV RECORDING IN OPERATION IMAGES ARE BEING MONITORED FOR THE PURPOSE OF PUBLIC SAFETY CRIME PREVENTION AND DETENTION AND PROSECUTION OF OFFENDERS This scheme is operated by For further information contact e	This may be used on a select few places in the city, usually on the main pole of the location where multiple cameras are installed. Text should be in Marathi in majority of places.
D	 24 HOUR CCTV RECORDING IN OPERATION IMAGES ARE BEING MONITORED AND RECORDED FOR THE PURPOSE OF CRIME PREVENTION AND FOR THE SAFETY OF THE PUBLIC THE SCHEME IS BEING OPERATED BY CONTACT DETAILS HERE	This is an alternative to type C.

4.18.17 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 Kakinada City Authority & its Consultant prior to the Go Live date.


Ticket Transfer Process
User
L1 Helpdesk
L2 - Vendor helpdesk
Report issue
Open Ticket 1 and assess vendor support
Forwards issue at L2 helpdesk
Update Ticket 1 and confirm closure with user
Close Ticket 1
Open Ticket 1
Call the user and take user requirements
Assign Ticket 2 to support team
Follow Incident Management Process to resolve the issue

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

4.19 ICT Enabled Solid Waste Management

4.19.1 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 four wheelers (loaders) carries the waste to the single location called waste processing plant. Also, Authority has field staff 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 management 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

4.19.2 Scope of Work

1. Business Solutions

The SI shall be responsible for Supply, Design, Development, Testing, Implementation (as per the functional requirement specifications mentioned in the RFP document), Operation and Maintenance (5 years) of ICT based Solid Waste Management System which includes:

ICT Interventions	Key Features
	a. GPS tracking of the waste pick up vehicle for real time tracking b. Route Optimization which shall help in reduction of trip

Solid Waste Management System	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/QR based 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 above should comply with (a) published latest e-Governance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in; and (b) leading industry standards and/or as per standards mentioned at Annexure –XI.

I. 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 the 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 leverage on the advanced GPS and GIS technologies for route scheduling, route monitoring, reporting and providing a quick dashboard.

II. RFID/QR code 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.

III. 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 Kakinada City operation center 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.

Ultrasonic or IR based level sensors to be provided to allow the system to identify the fill level and empty levels in a percentage basis and thereby garbage collection can be scheduled as a function of fill levels at different locations in the City.

Foul smell detection sensors/ Animal repellant sensors to be installed at select locations to the garbage bin to detect the quality of air being released into the atmosphere.

IV. 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 Kakinada City operation centre for report generation and alerts.

V. Mobile Device Software Specifications:

The Software should support applications such as:

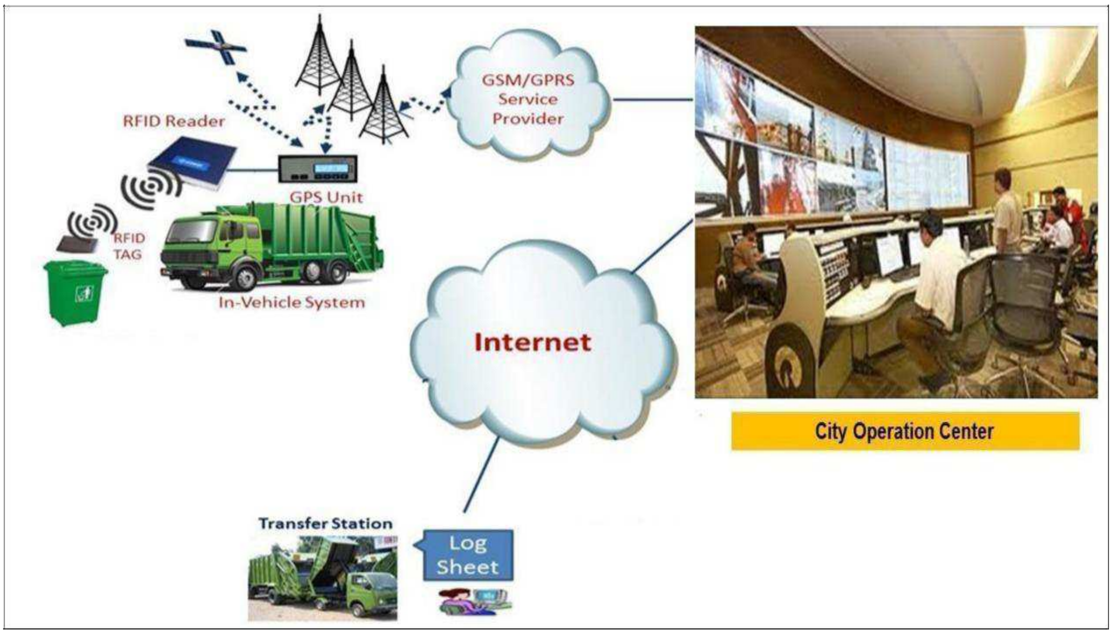
a. QR Code scanning
b. Job completion description
c. Crowd sourcing application for compliant registration and grievances

VI. 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
e. CCTV Cameras at Secondary and Final Dumping sites
f. Network connectivity for vehicles, bins to Kakinada City operation center

ICT Based Solid Waste Management System Schematic Solution Overview



4.19.3 Functional requirements 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.

Roles	Users
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	GPS, GIS

Roles	Users
schedule.	
Record of cleaning of roads / boundaries done as per schedule	GIS
Record of waste gone to process plant as per schedule	GIS, GPS
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
E] MIS	
Monitor the deployment of pickup trucks and personnel based on the schedule originally drawn.	GIS, GPS
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.	
Comparison of expenditure on SWM activities over different geographical areas, years, agencies, etc.	GIS, GPS, Accounts
Daily/Monthly reports of comparison for how much garbage to be lifted as per target & how much garbage is actually lifted. If less lifted then reasons for the same like 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	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

4.20 Smart Lighting

4.20.1 Overview

Certain streetlights have been identified which are to be replaced with Smart LED streetlights/floodlights. In case LED Street Lights are replaced in certain locations, these lights are also to be integrated with intended Smart Light System. Currently, existing traditional street light system is facing issues like:

1. Lack of information about the real time status of the street lights and area.
2. Lack of proper system for monitoring and operating lights ON/OFF schedule
3. Lack of system to optimize the efficiency of street light system as per requirement
4. Managing the independent unit of street light in terms of turning ON/OFF, fault detection and replacement etc.
5. Lack of system to enhance security by lighting dark areas in human presence
6. Lack of centralized system to view energy consumption, current light status and real time map based visualization
7. Lack of system to get inputs from other sources to customize control

The Authority intends to implement an energy efficient LED based Street Light System bundled with motion & ambient light sensors along with Smart controllers within the existing landscape to:

1. Minimize energy usage
2. Operate the street lights in three state (Dual DIM/Bright/Off) automatically as per the real time field requirement
3. Automated controls that make adjustments based on conditions such as occupancy or daylight availability
4. Policy driven central controlling mechanism to regulate the street lighting intensity and energy consumption
5. Real time tracking and management of street lights
6. Automatic illumination adjustment based on human presence by triggering multiple lamps to surround the person with a safe circle of light
7. Automatic status updates or failure alerts to remote server
8. Learn the existing occupancy pattern and predict occupancy patterns for future planning

4.20.2 Scope of Work

Business Solution

The SI shall be responsible for Supply, Design, Development, Testing, Implementation (as per the functional requirement specifications mentioned in the RFP document), Operations and Maintenance for a period of 5 years for Smart Light Management System which includes:

ICT Interventions	Key Features
Smart Lighting	LED base Smart lighting to support automated lighting and sensing
	Ability to control individual Outdoor LED lights on the street for turning on, off and dimming
	Ability to create policies for Outdoor City lighting based on time of the day, ambient lighting conditions and other scenarios and events on the street
	Monitor voltage, current, voltage fluctuation, power consumption for each individual light as well as a group of lights and City areas
	Detect failures of LED bulbs and other circuitry and generate alarms for maintenance automatically.

ICT Interventions	Key Features
	Enhance security by lighting dark areas in human presence Intelligent weather adaptive lighting control
	Learn occupancy pattern and predict the occupancy patterns for future planning
	Crowd sourcing or defective light reporting

The standards for above should comply with (a) published latest e-Governance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in; and (b) leading industry standards and /or as per standards mentioned at Annexure –XI.

Smart Lighting Operation Management System –

The system shall provision for:

a. Individual switch on/off, increase/decrease luminosity as per ground situation
b. Policy based Operation 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 day lights
c. Real time status of the Smart Lighting System on a Kakinada map view of Lighting Operations Management software
d. Automatically switched on /off on the basis of lux level. There should be a manual override and it should be monitored when used.
e. Amount of electricity used in street lighting. There should be information about the amount of natural lux levels and that created by the street lights on a 24 X 7 basis. This analysis would help Authority for allocating the amount of power required for street lights. The same analysis would also be used for changing the source of power to solar power in future.
f. Lux levels along with camera's on the street as well as capacity management report to help analyze if any Light has fused before time (before burn hours as specified in the supplier’s documentation.)
g. Policy based Operation 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 day lights, enhance security by lighting dark areas in human presence, time based scheduling with intelligent weather adaptive lighting control.
h. Learning occupancy pattern and predict occupancy status for future planning.

Infrastructure Solution

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. LED based Smart lighting fixtures with all fittings & fixtures (Motion & Ambient light sensors)
b. Smart Controllers mechanism
c. Network connectivity for street light poles, high masts, controllers and Kakinada City operation center

4.20.3 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 WiFi 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
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

#	Specifications
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

4.20.4 Smart Street Light Solution

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.

#	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
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

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)

#	Minimum Specifications
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

#	Minimum Specifications
	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%

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

#	Specifications
	by POWER DISTRIBUTION COMPANY and a sign-off on the same shall be obtained from POWER DISTRIBUTION COMPANY prior to finalizing the specifications; • Energy Meters shall be tested, installed and sealed in accordance with procedures specified by POWER DISTRIBUTION COMPANY; 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.	SI 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 SI 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, 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 SI 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

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, Dim 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)
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 of 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.
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 vapour lamp

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

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%

4.20.5 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

#	Specifications
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

4.20.6 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%

4.21 Smart Traffic

4.21.1 Overview

Majorly, Kakinada is having a large proportion of four Arm traffic junction just like every other Indian City.

Currently, the City is lacking advanced ICT enabled Traffic Management and Communication tools/systems. It is faced with a few problems like:

1. Traffic congestion and huge waiting time
2. No right of way to emergency vehicles like ambulances, police jeeps, fire engines, etc.
3. VIP movement clearance
4. Lack of information on prominent & frequent traffic congestions both location wise and time wise
5. Absence of street level public information & communication channel
6. Absence of central control mechanism to monitor & regulate the Kakinada traffic flow

Authority intends to implement a Smart Traffic Management System within the existing landscape to:

1. Automate the process of traffic management by optimally configuring the traffic junction lights on real time basis
2. Minimize the traffic congestions and waiting time
3. Centrally controlled traffic management system to ensure smooth movement of emergency services like ambulance, police etc.
4. Managed & coordinated VIP movements
5. Availability of traffic data to further analyze and optimize the traffic flow
6. Real Time Incident Message and Advisory Messages to citizens
7. Improved Traffic Regulation

4.21.2 Scope of Work

1. Business Solution

The SI shall be responsible for Supply, Design, Development, Testing, Implementation (as per the functional requirement specifications mentioned in the RFP document), Operation and Maintenance (5 years) of Smart Traffic Management System which includes:

ICT Interventions	Key Features
Smart Traffic	Adaptive Traffic Management System
	Public Announcement System
	Variable Message System

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

I. Adaptive Traffic Control System (ATCS) –

ATCS shall offer traffic signal optimizing functionalities, use data from vehicle detectors and optimize traffic signal settings resulting improved vehicle delays and stops. The system shall also allow interconnecting individual area controllers and thus enabling traffic monitoring and regulating functionality from the central location.

The primary objective of the system is to monitor and control traffic signals, including signalized pedestrian crossings, using a traffic responsive strategy based on real time traffic flow and vehicle presence information. However, the system shall also be capable of operating under isolated vehicle actuated plan.

All junctions under Adaptive Traffic Control System shall be provided vehicle detection system & communication equipment. This shall allow each intersection controller to be monitored from central control for proper functionality. Any corrective action can be initiated either automatically based on status information or by an operator. The real time detection data shall be communicated to the central control station by each controller.

ATCS shall be driven central control system, on real time basis, with the capaKakinada to calculate the optimal cycle times, effective green time ratios, and change intervals for all system traffic signal controllers connected to it which in turn can also work in configurable manner. These calculations shall be based upon assessments carried out by the ATCS central application software running on a Kakinada Operation Center based on the data and information gathered by vehicle detectors at strategic locations at the intersections controlled by the system

Health Monitoring should also be available for the traffic lights with Auto / manual mode of controller, Flash mode or normal mode, Power interruption, Intrusion in controller, Aspect monitoring of traffic lights.

The solution should include following minimum reports:

- Stage Timing report
- Cycle Timing report
- Stage switching report
- Cycle Time switching report
- Mode switching report
- Event Report
- Power on & down
- Intensity Change
- Plan Change
- RTC Failure
- Time Update
- Mode Change
- Lamp Status Report
- Loop Failure Report
- Conflict
- Corridor Performance Report
- Corridor Cycle Time Report

The SI may also be requested to generate additional reports as per Kakinada requirements.

4.22 Smart Parking

4.22.1 Overview

Residents of *Kakinada city* are facing trouble in finding parking space and frequently they are facing change problems for parking fee payments. With Smart Parking solution that alerts residents on the details of availability of parking space and also enables to pay requisite fee with mobile wallets or bank wallets or mobile wallets like payTM, etc.

Challenges with Conventional Parking:

1. High Parking Search Time
2. Traffic Congestion on Road due haphazard parking
3. Poor Usage of Parking Space
4. Poor Occupancy in Parking Lot
5. Less Revenue / collection
6. Less effective parking operations
7. High Parking violations
8. Accidental Hazards
9. Stress to user & dissatisfaction
10. Pollution – High Emission of gas
11. No flexibility in Parking Charges
12. Suspicious parking / Lack of security arrangements in Parking
13. No real time tracking, data/report for analysis for future need/expansion

Value Proposition SMART Parking offers to its Stakeholders:

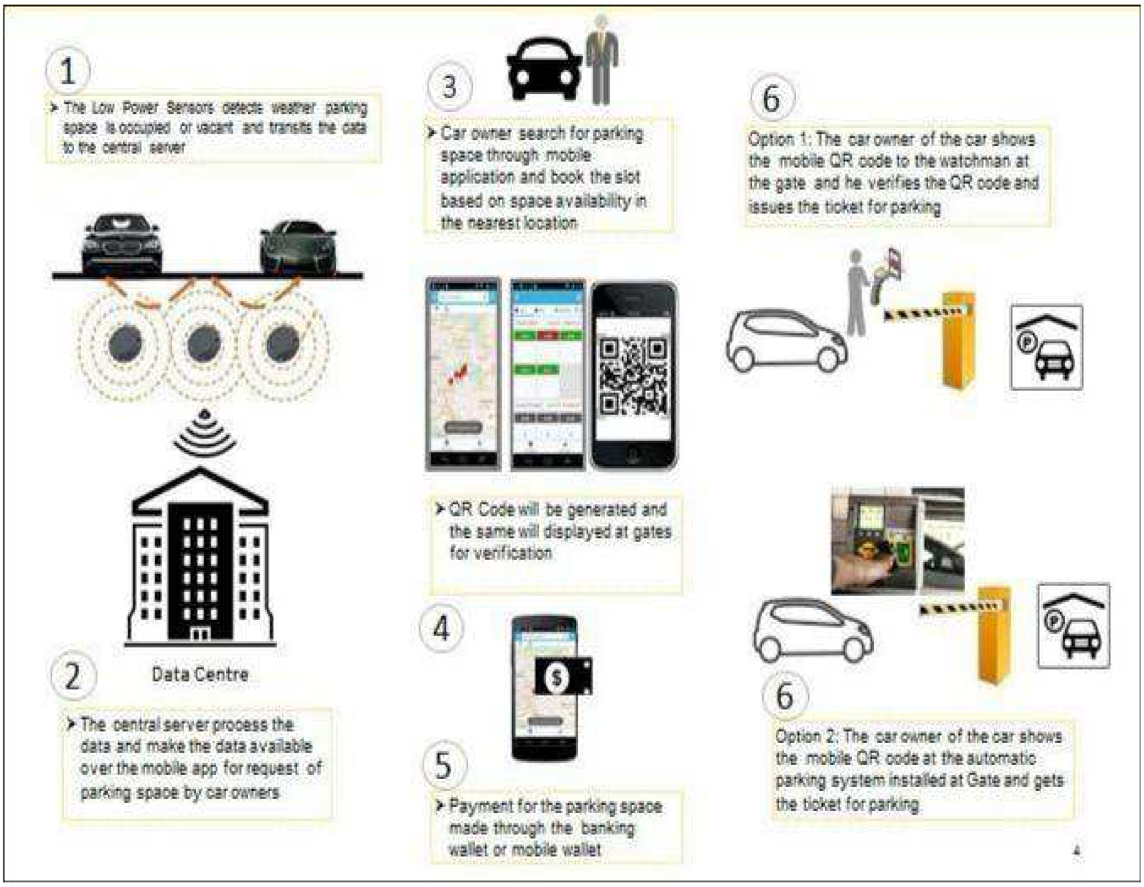
Authority	**Citizens**
1. Increase quality of life 2. Improvement in citizen's parking experience & satisfaction 3. More efficient use of parking 4. Reduces illegal parking 5. Reduces revenue leakages 6. Reduces Man power cost	1. Simplifies Payment 2. Easily finds the parking space 3. Time saving 4. Avoid traffic congestion

4.22.2 Scope of Work

SMART Parking – Solution & its Benefits:

1. Mobile App can help in finding parking space quickly & easily
2. Finding parking space with clear & simple directions reducing traffic Congestion. Parking violation detection real time system also help.
3. Assisting user in directing to correct parking slot help in correct parking at correct slot, making optimal usage of parking space
4. Real time update of entry & exit of vehicle improve occupancy
5. Improved Parking Occupancy increase collection
6. Ease of payment improve collection & save time
7. Real time info, Smart meters, ease of payment improve parking operations
8. Clear, simple directions & ease in parking reduces road accidents
9. Improved user satisfaction by saving time, effort & cost
10. Less parking search time reduces emission of gases & control pollution
11. Provision for demand responsive parking charges – Higher charges during peak hours, etc.
12. Correct detections of violations & suspicious parking/over duration parking
13. Data Analysis to look into status of utilization of parking space-sufficient, insufficient for planning future expansion plans of parking slots, revenue generated; subsequently required measures to be taken to handle parking problems

Smart Parking Solution Requirement Overview



1 ➤ The Low Power Sensors detecte weather parking space is occupied or vacant and transits the data to the central server

2 ➤ The central server process the data and make the data available over the mobile app for request of parking space by car owners

3 ➤ Car owner search for parking space through mobile application and book the slot based on space availability in the nearest location

➤ QR Code will be generated and the same will displayed at gates for verification

4

5 ➤ Payment for the parking space made through the banking wallet or mobile wallet

6 Option 1: The car owner of the car shows the mobile QR code to the watchman at the gate and he verifies the QR code and issues the ticket for parking

6 Option 2: The car owner of the car shows the mobile QR code at the automatic parking system installed at Gate and gets the ticket for parking

1. Installation of sensors in each bay, which register whether the bay is occupied or vacant.
2. This information to relay live to local and central system where parking management application is hosted, which collates and analyses the data.

   Then this information is relayed instantaneously to signage & digital-display screens which let customers know how many spaces are available and give directions for locating them, throughout the car park, until the driver arrives at a vacant space

4.22.3 Key Components

1. **Parking Sensors**
   1. Installation of parking sensors in the allotted space which communicate information wirelessly on the occupancy of parking lot or vacant lot after a vehicle leaves the parking lot.
2. **Wireless Sensor Networks Module**
   1. Collect sensor data
   2. Check parking slot status in real-time
   3. Send parking slot information to embedded webserver
3. **Embedded Web-Server**
   1. Receive parking slot status information from wireless sensor networks
   2. Send them with the position of parking zone to central web-server
   3. Generate ticket of the mobile users via QR code reading
   4. Allocate parking space to local users and generate ticket
   5. Integrated with local display unit and boom barrier
4. **Mobile Device of Driver**
   1. Connect to central web-server
   2. Receive parking slot information from central web-server
   3. Display the real-time monitoring of parking slots state in the nearest parking zone

5. **Central Web-Server**
    1. Receive parking slot information from embedded web-server
    2. Display the parking slots state of parking zone in real-time
    3. Send information to mobile phone application
    4. Save information in SQL or equivalent database
    5. Reporting & analytics
6. **Boom Barrier & Digital Display Unit**

    Shall receive information from the Parking Information System and operate accordingly. The standards for above should comply with (a) published e-Governance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and (b) be of leading industry standards and /or as per standards mentioned at Annexure –XI.

4.22.4 Parking Management System: Functional Requirements

1. **Entry Requirement**
    - i. Entry to any parking space should have outdoor displays/screens showing overall availability of parking slots in that particular parking space.
    - ii. Each entry lane should be equipped with one Entry Device with the following capabilities:
        - a) The Entry Device should act as an Automatic Ticket Dispenser
        - b) It should have touch screen for motorist to enter Unique Booking Number
        - c) The Entry Device should have Near Field Communication (NFC) capability
        - d) The Entry Device should have capability to connect with Intercom, microphone, speaker and other subsystems
    - iii. The ticket, QR Code and Smart Parking Card or any other technology used by SI should be capable of capturing data that is easily retrievable at the exit.
    - iv. Every vehicle entering the parking space should be stopped by barrier. The barrier is raised when the motorist is issued a ticket or has been identified as a legitimate user.
    - v. In case the parking lot is already occupied to its capacity, the ticket issuing should automatically be blocked and therefore, the barrier should not open. A message should also be displayed on the outdoor screen stating the same.
    - vi. The Entry Device should be able to detect and report:
        - a) Anti-pass back
        - b) Back-out ticket
        - c) Low ticket stock
    - vii. The display on Entry Device should have capability to display messages in English, Hindi and other Regional languages.
    - viii. The solution should also include provision to capture the image of vehicle and license plate number of every vehicle entering any of the parking spaces using dedicated cameras.
2. **Exit Requirements**
    - i. Any vehicle, before leaving the parking area, should be stopped by a barrier system at the point of exit from the parking.
    - ii. The solution should have clearly instructed easy to use interface
    - iii. The solution should also include provision to capture the image of the vehicle including license plate number exiting any of the parking spaces and the all the information related to the same should be stored at a central server.
    - iv. Manual Pay Station:
        - a) Exit of every parking should be equipped with a manned Pay station (booth).
        - b) The exit booth should have appropriate space for keeping devices such as a computer with internet connectivity, QR code reader, credit card reader, printer etc.
        - c) For motorists who enter the parking lot using Smart Parking Card, Monthly pass or any other NFC capable card provided by SI, the exit booth should also have NFC facility for motorist to tap his/her Smart Parking Card for express exit.

The payment can also be linked to the e-Wallet of the motorist with auto-debit option and corresponding limits and alerts to the same.

d) The personnel monitoring the exit Pay Station is also required to manually enter the License number details in the system so that the license number, along with date and time of exit, is stored in the database.

e) The payment for parking should be collected based on entry time stamp by any personnel stationed at the Pay Station.

f) The system will calculate the fee automatically and indicate this on the screen clearly visible to the motorist. No manual intervention should be necessary to compute the fee.

v. Once the vehicle exits a parking slot, the total parking slots available in that parking space should automatically get updated.

vi. Only after completing the full cycle correctly the transaction will be considered as valid within the car park. However, audit trail of each complete, incomplete and cancelled transaction should be available in the system

vii. The solution should be equipped with Anti-pass back technology and be able to detect and report any instance pass back.

viii. The solution should allow full integration of third party devices with the Parking Management and Guidance System, and capture all transactions to generate customized reports.

ix. The solution should track each and every revenue source and should ensure no leakages due to manual intervention.

x. The Pay Station should be capable of charging devices.

3. Entry and Exit Barrier

i. The entrance and exit of each parking lot should have a barrier gate system using technologies such as boom barriers, bollards etc.

ii. The barrier should remain in open position for optimal period of time for the vehicle to pass at entrance and exit.

iii. The solution should also include provision to capture image of vehicle including license plate number of every vehicle entering and leaving any of the parking spaces and the all the information related to the same should be stored at a central server.

iv. Barrier should have capability of in built glowing direction signage

v. Barrier Arms should have the following options:

a) In closed position the full arm should be illuminated red.

b) During movement the full arm should be illuminated yellow

c) Once reached open position the full arm should be illuminated Green.

vi. Upon horizontal impact by a vehicle, the barrier arm should get detached from the barrier unit with minimal damage to the vehicle and the barrier motor mechanism. An alarm should also be raised and sent to the server and monitoring console, when the barrier is detached.

vii. An alert should be sent to the console and server to ensure that the administrator is informed that the barrier is not attached or barrier breakage.

viii. All vehicular passages during the time that the barrier is not attached should be recorded and displayed in the reports separately in order to audit the necessary revenue transactions during that time.

ix. Upon impact during closure, the arm will stop and stay in the same position. Under no circumstances should the arm re-open upon impact. This is to prevent keeping the arm open for illegal entries or exits.

x. The barrier arm should be easy to refit with barrier unit in a short duration (within one minute).

xi. If for any reason and external override (fire system) needs to be connected, then this should only be possible over the Entry/exit Device and the switch should be permanently monitored by the Parking Management System.

4. Wireless Handheld Device

The solution should include the use of wireless handheld device for on-street and off-street parking. This device shall be used in case of street parking or indoor parking or open parking during peak hours or as a fallback mechanism. However, this device must track every transaction limiting any manual transaction to zero.

i. **Street Parking Mode**:

a. It should be possible to use wireless handheld devices in street parking model.

b. On arrival of motorist, it should be able to dispense a ticket

c. The same device should also be able to function as cash register

d. The transactions should get uploaded instantly and automatically to the central parking management system using online connectivity.

ii. **Indoor or Open Parking Mode:** In case of high traffic at any of the parking lots or during peak hours, it should be possible for the wireless handheld device to be used as central cashiering device (i.e. it should be possible to scan the QR Code on tickets issued by the entry device and issue receipts post payment, so that the motorists could pay for the parking and then drive out quickly), without any time consumed for payment transactions at the exit.

iii. The device should have capability to print parking receipts and bar coded tickets in real time.

iv. Both the functionality of ticket dispensing & cash register should be possible to be combined in one device.

v. This wireless handheld device should be an online unit, connected in real-time with Command and Control Centre using either Wi-Fi or GPRS. However, in case of network failure, the device should have capability to transact offline and sync with the server as and when connection is restored.

vi. The wireless device to have batteries and power supply along with cradle for charging.

5. Payment options

i. The primary mode of payment for parking will be by cash at the Pay Station

ii. For bookings through Citizen App or Smart Web portal application, payment will be made using e-Wallet, net banking, credit card, debit card etc.

iii. Additionally, the SI can implement innovative and cost effective payment methods (such as e-vouchers).

Parking Guidance subsystem for motorists

1. Sensors for vehicle detection

i. The sensor should be intelligent and accurately detect if the car space is vacant or occupied.

ii. Appropriate sensors should be chosen based on the type of the parking spot and its external conditions. The preferred sensors would be geo-magnetic sensors, but the SI can propose innovative, advanced but reliable implementation approaches using other sensors.

iii. The sensor should be able to detect a vehicle irrespective of the depth or height of sensor installation.

iv. Each sensor should have its own unique identification in order to be accurately tracked by the Parking Guidance System.

v. Each sensor should have an accurate and real time feedback mechanism to be detected automatically by the system in case of faults.

vi. It should be placed appropriately per parking spot.

2. Parking aisle light indicators

i. Light indicators should be installed for all indoor parking lots for motorist to see the available and occupied spaces from the parking lane easily

ii. Once a parking spot is occupied the total parking slots should automatically get updated.

iii. The fixation of the light indicators to the ceiling should be easy and fast, and should use a quick fastening clips to easy the installation.

iv. The SI may suggest any similar innovative solution for Open Parking and Street Parking.

3. **Informative Display Panels**
   i. The display panels units should indicate available spaces for each parking aisle, bay/zone/level, total parking and should be able to be customized by software.
   ii. The display panel should be easy to understand and must have graphical directional and zone status indication (as red crosses for zone full or green directional arrows to guide drivers to zones with available spaces).

4.22.5 Smart Parking apps for Citizens

The Citizen App and Web Portal are required as a part of Smart Parking Solution.

a) Vehicle and License Plate Image Capture

i. The solution should have capability to automatically capture details of the license plates of the vehicles at every entry and exit of each parking lot.

ii. The image should be clicked at the entry point when the ticket is issued and at the exit point during payment. The image of the license plate should be linked to the details of the corresponding ticket issued in real- time and stored in the database for one month. This information will be stored in the Kakinada operation Centre.

iii. The system checks daily whether the vehicles that have entered the premises but are yet to leave. Thereby Parking management and Guidance system(PMGS) can generate alert if any vehicle is overstaying in the parking lot over 24 hrs.

iv. The SI shall install appropriate cameras at entry and exit of each Parking Lot.

b) Provision for Smart Card

i. Along with the paper ticket, the SI can propose a cost effective smart parking solution to include NFC enabled Prepaid Smart Card system for premium customers and customers opting for monthly reserved parking passes.

ii. The NFC enabled smart card reader would be available at Pay Station and would automatically deduct the required payment towards parking.

iii. NFC enabled smart card solution is implemented, its devices should be able to communicate to the centralized Command and Control Centre, to transmit all parking related information back and forth.

c) Real-time Monitoring and Dynamic MIS Reporting

i. The system should include central reporting system establishing the connection between the devices and sensors, and the centralized Command and Control Centre.

ii. The solution should include reporting dashboards with location specific thresholds to be set for generating customized reports

iii. The solution should be capable of monitoring the number of vehicles that entered or exited the parking premises during any given time

iv. The solution should generate reports for each parking spot, in each of the parking lots capturing utilization, cost, and revenue details, and details of assets, people and etc.

v. These reports should be available in all standard acceptable formats like .csv, .pdf, .txt, etc.

4.22.6 Technical Requirements

1) Sensors:

i. Sensor should be used for detecting the real-time status of the parking space.

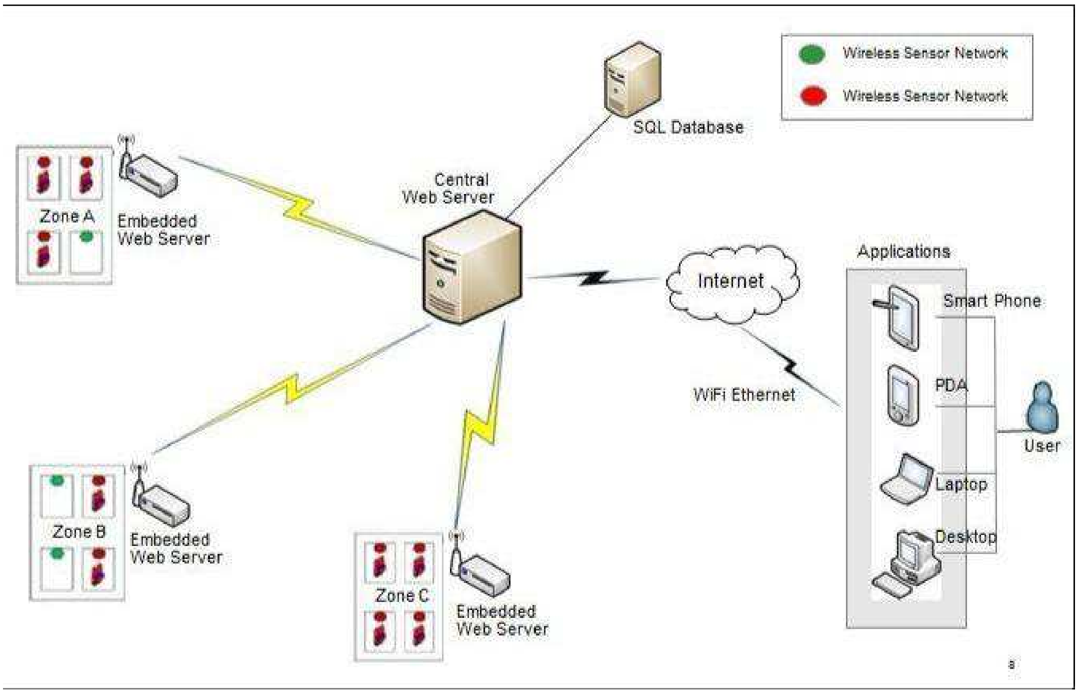
ii. It should be able to upgrade its firmware functionality remotely from the centralized Command and Control Center.

iii. It should be able to permit an optimal angle between the sensor output and the target.

iv. Sensors should be able to work in all weather conditions relevant to the project site.

v. Sensors should preferably have magnetic and optic technology

Smart Parking Technical Architecture



2) **Parking aisle light indicators**
   i. This feature should be available for indoor parking lots
   ii. The light indicators for external view should be high intensity LED which helps the motorist to see the available spaces from the parking lane easily
   iii. The preferred parking aisle indicator should be visible from all directions for traffic, and have high intensity LEDs.
   iv. Once a parking spot is occupied and the indicator must turn red, the total parking slots available in that parking space should automatically get updated.
3) **Indoor LED Display**
   i. The display panels should have high intensity LED.
   ii. The display panels units should receive information directly from same communication line and its update time should be less than 5 seconds to increase/decrease any car availability value.
   iii. The display panel should have optional numerical length, i.e., according to each parking, it should be possible to display up to 4 digits
4) **Corner protectors**: Rubber matting with Black and yellow stripes with Installation
5) **Bumper**: Stripped Teflon coated Bumpers at entry, exit and aisles of parking lots

4.23 Environmental Sensors

4.23.1 Overview

Environmental pollution, particularly of the air, is nowadays a major problem that unknowingly affects lives in the cities. As clear focus of building *Kakinada city* as one of the finest example of Smart Kakinada City solution, Authority believes it is important that citizens know of the air that they breathe. *Kakinada city* Citizens & visitors to *Kakinada city* can enjoy unique experiences that keep them feeling good by knowing Kakinada's environmental conditions at different locations. The Air quality should be monitored by a network comprising of:

- fixed monitoring stations
- Data processing
- Data transmission to a central system
- A central processing system

4.23.2 Scope of Work

The SI should

1. Install environment sensors (as per the functional requirement) to display environment related information at various strategic locations through variable message system
2. The environment sensors shall be integrated with the central control system at Kakinada City operation center to capture and display/ provide feed on Temperature, Humidity, Pollutants like SoX, NoX, CoX, etc., PM2.5, PM10, Noise Pollution, Electromagnetic Radiation etc. The data it collects is location-marked.
3. 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.
4. Then this information is relayed instantaneously to signage – large, clear, digital-display screens which let citizens know regarding the prevalent environmental conditions.
5. Further environmental sensors recorded data shall be used by Smart Environment Mobile application to enable user for alarm management and notification of environmental details on real time basis.
6. Develop mobile app for Grievance Redressal of Citizen – where citizen can take the picture, upload the same with Geo Tagging. The complaint should be automatically forwarded to the respective staff, with escalation within specified timelines supported with multilingual text to speech, speech to text and speech to speech systems.

4.23.3 Components

1. **Wireless Environmental Sensor**
   - Collect sensor data
   - Send recorded information to central system
2. **Central System**
   - Receive information from environment sensors
   - Display the information on real-time basis
   - Send information to mobile phone application
   - Save information in database
3. **Mobile Device of Driver**
   - Connect to central web-server
   - Receive environment information from central system
   - Alarm management and safe environment mode features
4. **Digital Display Unit**
   - Shall receive information from the central application System and operate accordingly

4.23.4 Functional requirements:

- They should be ruggedized enough to be deployed in open air areas on streets and park
- They should be able to read and report at least the following parameters
  - Temperature
  - Humidity
  - Ambient Light
  - Sound
  - CO
  - NO2
  - Mosquito density
- The sensor should be able to communicate its data using wireless technology
- The data should be collected in a software platform that allows third party software applications to read that data.
- The sensor management platform should allow the configuration of the sensor to the network and also location details etc.

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 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.

4.23.5 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

The standards for above should comply with (a) published e-Governance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and (b) leading industry standards and /or as per standards mentioned at Annexure –XI.

4.24 Smart Governance apps for Citizen Services

4.24.1 Overview

Smart Governance captures the important attributes of Good Governance i.e. Simple, Measurable, Accountable, Responsive and Transparent governance. ICT in governance has been experienced in the form of e-Governance, which redefined the way Governments work, share information, engage citizens and deliver services to external and internal clients for the benefit of both government and the clients that they serve. Governments harnesses information technologies such as Wide Area Networks (WAN), Internet, Intranet, World Wide Web and mobile computing reach out to citizens, business, and other arms of the government to: Improve delivery of services to citizens, businesses and employees. Engage citizens in the process of governance through interaction. Empower citizens through access to knowledge and information and Make the working of the government more efficient and effective. Results in enhanced transparency, convenience and empowerment; less corruption; revenue growth; and cost reduction.

4.24.2 Solution Requirements

The components envisaged to be included in Smart Governance are:

a. Stamp Duty & Registration
b. Tracking and monitoring of Taxes Collection
c. Online Management Monitoring and Accounting System
d. Works & Account Management System
e. Web based Land Management System
f. Legal Management
g. Document Management System
h. Human Resource Management System
i. Intelligent Script Manager
j. Speech to Text
k. Multi-lingual interfaces
l. Schemes Management, etc.

The features under Citizen Services shall include the following:

a. Grievance Redressal System
b. Universal Identity (Aadhaar)
c. Multi-purpose Smart card
d. Utility Services
e. Public & Digital Library
f. Women & Child Safety
g. Welfare Schemes
h. Assistive living for differently abled
i. Property Tax
j. Registrations & Certification
k. License Facilities
l. Tourism & Heritage, etc.

The standards used for the above should comply with (a) published latest e-Governance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in; and (b) be of leading industry standards and /or as per standards mentioned at Annexure –XI.

4.24.3 Scope of Work

The SI shall ensure that all the module under Smart Governance is integrated with the overall project. SI shall create enabling platform to link the relevant features with the Citizen Centric Services. [*the SI shall be responsible for developing the Smart Governance solutions for the Kakinada City and link the same with the citizen services.* The Smart Governance shall consist of following solutions:

a. Stamp Duty & Registration (GAURI, KAVERI, SARITA)

A model of the BPR to reorient the Department of Registration and Stamps towards 100% automation in the registration process and speedy delivery of registered documents to the citizens. The application suite shall consists of:

- Registration Module
- Valuation Module
- Reports Module
- Vendor Management System (VMS)
- Utilities Module
- Societies, Firms and Marriage Registration Module
- Scan-Archival Module
- Data Transmission Module
- Website

b. Online Management Monitoring and Accounting System

OMMAS, a web based online system for the monitoring of schemes to be established so that all the information related to Release of Funds, Utilization of Funds, Status of Progress of work and quality monitoring reports are available to citizens & govt. officials for viewing & analysis. OMMAS would assist the department officials in:

- Preparing the Proposal from the Core Network, scrutinizing by the State Technical Agency (STA) and sanction from respective department
- Capture the monthly physical and financial progress of the work
- Monitor the quality of the work under three stages i.e., In-Progress, Competed and Maintenance by State Quality Monitors (SQM) and National Quality Monitors (NQM)
- Quality of work is monitored using the Mobile based application enabling the monitor to upload the real time photographs of the roads right from the inspection site.
- Accounting modules helps to manage the funds transferred from Ministry of Rural Development to the State Executing Agency and account for the usage of funds in the implementation
- Accounting module also enables to capture the work wise expenditure
- All the accounting reports like Cash Book, Ledgers, Balance Sheet, Schedules, Registers and Monthly Account are generated after monthly closing based on simply posting Receipts and Vouchers.
- Works under maintenance can also be monitored based on periodic inspection of the Pavement Condition Index of the roads

c. Works & Account Management System

Works Management System – an integrated package for Designing, Estimation, Execution, Monitoring & Tracking of Civil Engineering Construction Projects. The key features of the solutions are:

- To generate electronically Contractors Bills, Budget estimates, Monthly Accounts and book keeping as per the statutory governmental procedures.
- Tracking, Processing, Consolidating and Reporting of Financial transactions

- Near real-time Assessment of Expenditure against the Grants/Allotment received as per the budget
- Assess Physical progress of various projects undertaken by the department with regards to the financials.
- Increase the efficiency of individual functional wings of the department.
- Achieve integration with the systems of other line departments/Nodal Agencies such as the AG and the treasuries for submission of data digitally and achieve online reconciliation.

d. Web based Land Management System

Web-based enterprise GIS solution which enables the Authorities / Government, Landowners and Public to access and share requisite information with high level of security and data integrity. The system shall incorporate facility to dole out compensation and enhanced compensation information along with the legalities involved in their business process. It involves scanning, digitizing and geo-referencing of the Village Maps, Layout Plans, Master and Land Use Plan. The spatial data and non-spatial data together with the developed application tools and GIS interface has helped the Administration in various aspects like perusing plot information, finding plot of land to be acquired and maintaining the detailed information with high level of integrity. The web enabling capability has enabled the common citizen to access information related to their plot of land through the Internet.

e. Digital Repository

The objective of the solution is to create Trustworthy Digital Repository (TDR) a long term digital preservation environment for the disposed case records through adaptation of Open Archival Information System [OAIS (ISO14721:2003)]. The key features shall be:

- Tracking of workflow of documents and Users
- Correspondence Management
- Customizable Office Filing Environment
- Document Approval and Sign-off Sheet
- Document linking and annotation
- Document Monitoring
- Alerts & Reminders
- Report Generation Tool
- Access Rights Management and Control
- Profile Creation & Management
- Information Extraction, Search & Retrieval
- Graphical/Statistical representation of Information
- Automatic Summarizer
- Security Overlay

4.25 Legal Module

Roles	Users
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, Web, Intranet
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/ advocate/Officer)	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	

4.26 Document Management System

A Natural Language Processing based Document Management System to manage documents data throughout their lifecycle, right from inception stage through creation, review, storage and finally disseminate all the way to their destruction. The key features shall be:

- Social networking for Enterprise / Organization
- Individuals, Groups, Events areas (based on templates)
- Integrated calendar, activity stream, dashboard, and more
- Communicate ideas, information, events, artefacts
- Through use of pages, blogs, forums, files (image, document, video)
- Through interactive chat
- Powerful framework to build behaviour-analytics, data analytics, etc.

4.27 HRMS (Human Resource Management System)

The HR function consists of tracking existing employee data which traditionally includes personal Information, Skills, Salary, Leave, Tour Claims, Medical Claims etc.. To reduce the manual workload of these administrative activities, customized Human Resource Management System can be created. Key features shall be:

- Rule based Access control
- Work Flow
- Configurable Policies
- Payroll and Income Tax
- Provident Fund
- Leave Management
- Travel Bills
- Reimbursements
- Pay-slips
- Attendance tracking
- MIS Dashboards etc.
- School Information System comprising of Teacher & Student Performance, School Buildings, Smart Schools, Tracking and monitoring of Schemes, like Mid Day Meal Scheme, Sarva Shiksha Abhiyan, Scholarships, etc.

4.28 Hospital Management System

Roles/Responsibilities	**Users**
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	

Roles/Responsibilities	**Users**
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	
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 anaesthesia 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)	GIS
Case details, Location, 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 tests 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

Roles/Responsibilities	**Users**
Issuance of certificates (Templates to be prepared for issuing fitness/unfit certificate)	HRMS
I] Student Management	HRMS
Attendance	
Shifts	
Posting of students	
Training Certificate	
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	

4.29 Welfare Schemes Module

Roles and Responsibilities	**Users**
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	Web Portal

Schemes, Contributory Health schemes, ICDS immunization Programs, Integrated child development project, Any other Schemes	
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	

4.30 Project Systems (Engineering) Module

Roles	Users
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	Intranet
E] Tendering	

Roles	Users
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	
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	

Roles	Users
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, Building Permission Module, Grievance Redressal Module, Alerts for Road Re-surfacing / Repairing	GIS
Cross-departmental information as alerts while defining new projects, eg. : 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 Requirements	
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)	
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 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)	

4.31 Municipal Secretary Module

Roles	Users
A] Executive Wing Database	
Database of members of various committee, corporator, mayor, etc.	Web
B] Agenda Preparation	
Preparation of Agenda by Department & submission to Municipal Secretary Dept.	Projects
Submission of proposals from various Counsellors	
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
Distribution of Resolution	DMS
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)	

4.32 Asset Inventory Management

Roles	Users
A] Classification of Assets	
Immovable Assets – Land, Building, Roads, Footpaths, Bridges, Culverts, Flyovers, Subways & causeways; Drains including underground drains, Water Works Distribution, Public Lighting System, Lakes and Ponds, Capital Work-in Progress	GIS, Project Systems
Movable Assets- Plant and Machinery – including machinery of Water Works & Drainage, Road dept. machinery, Vehicles, Furniture & Fixtures, Office Equipment, Other Equipment, Live Stock	Stores
Investments	Accounts
Capture Various details for the Assets- Ownership, Cost Details (construction / Purchase / Transfer), Depreciation Principles, 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, Web
Acquisition of Land	
Asset Sale	
Investment on Assets (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

4.33 Land & Estate Management

Roles	Users
A. Land Management	
Proposal for Land Acquisition	GIS
Scrutiny of Land Details	Web, Municipal Secretary
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

4.34 Materials Management

Roles	Users
A] Masters	
Categorization of Stores - Central Stores, Central Medical Store (CMSO), Hospital Stores, Biomedical Engineering Store, General Stores (issuing stationery and non-medical materials), Electrical Stores, Civil Stores, Street Light Department Stores, Water Supply & Drainage Dept.,Roads & Building Dept., 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	Accounts
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 for reordering.	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	
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.	

Roles	Users
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.	Web, Procurement Module
Release vendor’s EMD	Web
Intimate vendor about receipt of materials at central stores	SMS Gateway

5.0. 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 have to be approved by Authority for the successful bidder to 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.

5.1 Implementation Plan

The service provider should prepare and submit a detailed plan during execution of order with following details as given herewith. 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

5.2 Network interfaces requirements

- 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

5.3 Disaster Recovery (DR)

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.

DR Management

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 Main Data Centre (MDC) 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:
  - o Key Processes automated by the application and key process owners
  - o Hardware and Software technology stack of application
  - o Identification of business activities of the processes including criticality, impact and dependencies
  - o 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 main 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.

5.4 Testing Methodologies

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 o 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.
- **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.

5.6 Configuration of proposed solution

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, HPUX, 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

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.

6.0 Smart Data Center

Data Center

- 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.

6.1 Technical Specifications

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
10.	QOS Features	RSVP Priority Queuing Policy based routing Traffic shaping Time-based Quality of Services Policy Bandwidth Reservation/Committed Information Rate

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, halfduplex 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 console term 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

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.

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

#	Specifications
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.

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
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

#	Parameter	Minimum Specifications
		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

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

#	Parameter	Minimum Specifications
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).

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.

#	Parameter	Minimum Specifications
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)

Core Router

#	Item	Minimum Specifications
1.	Multi-Services	Should deliver multiple IP services over a flexible combination of interfaces
2.	Ports	As per overall network architecture proposed by the bidder, the router should be populated with required number of LAN/WAN ports/modules, with cable for connectivity to other network elements.
3.	Speed	As per requirement, to cater to entire bandwidth requirement of the project.
4.	Interface modules	Must support upto 10G interfaces. Must have capability to interface with variety interfaces.
5.	Protocol Support	Must have support for TCP/IP, PPP, 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

#	Item	Minimum Specifications
12.	Security features	• MD5 encryption for routing protocol • NAT • URL based Filtering • RADIUS Authentication • Management Access policy • IPSec / Encryption • L2TP
13.	QOS Features	• RSVP • Priority Queuing • Policy based routing • Traffic shaping • Time-based QoS Policy • Bandwidth Reservation / Committed Information Rate

Internet 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

#	Item	Minimum Specifications
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

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
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

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
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

#	Parameter	Minimum Specifications
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

#	Parameter	Minimum Specifications
		• 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

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

Tape library

Sr No **Item**	**Minimum Specifications**	
1	Make	Must be specified
2	Model	Must be specified. All relevant technical information must be submitted
3	Technology	LTO 6
4	Number Drives	Two LTO 6 Drives
5	Media Slots	Minimum 45
6	Interface	Minimum 4 Gbps FC Interface
7	Power Supplies	Redundant Hot Swap Power supply
8	Fans	Redundant Hot Swap cooling fans
9	Software	Security and Remote Management Software
10	Supported Backup Software	Should support industry leading backup software such as 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

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

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 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 Fixtures

- 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 40character 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

- These specifications cover 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.), Canada
- 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 SI 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.

6.3 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

6.4 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

6.5 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.

6.6 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 standardization 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, Top N, 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.

7.0 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

7.1. Prepare & Access

Finalize 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.

Finalize 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.

Finalization 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.

Finalize 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.

Finalize 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 Kakinada 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.

7.2 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 finalized by Authority.

Finalize 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

Observation 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)

Integration of 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.

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

(a) Software development/customization based on the functional requirement specifications, system requirement specifications, software requirement specifications and solution designs as finalized 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 operationalization 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.

- 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.

Annexure I : Indicative List of Wi Fi Locations

Sl No.	Area Within Kakinada	# of Locations
1	Centres (As per list at Annexure II)	30
2	Schools & Office Buildings	100
3	Parks and other Important Locations	30
	Total	**160**

Annexure II
List of Existing Surveillance Locations

Name of the location of PTZ/CC	# of Cameras	IP Address
Annammaghati Centre	4	
Annammaghati Centre Towards New Bridge		
Annammaghati Centre Towards Charties		
Annammaghati Centre Towards RCPM Road		
Balaji Cheruvu Centre Towards Devalayam Street	**1**	
Balayogi Statue JN Towards Yanam Road	3	
Balayogi Statue JN Towards Charties Road		
Balayogi Statue JN Towards Mahalakshmi Road		
Jagannaikpur Old Bridge	5	
Jagannaikpur Old Bridge Towards Venkateswara Temple Road		
Jagannaikpur Old Bridge Towards Old Bridge		
Jagannaikpur Old Bridge Towards New Bridge Road		
Jagannaikpur Old Bridge Towards Yanam Road		
	1	
I Town PS Centre	5	
I Town PS Centre Towards New Bridge		
I Town PS Centre Towards Main Road		
I Town PS Centre Towards 1Town PS Center		
I Town PS Centre Towards Old Bridge		
Masjid Centre	5	
Masjid Centre Towards 1Town Raod		
Masjid Centre Towards Devalam Road		
Masjid Centre Towards Market Road		
Masjid Centre Towards 2 Town Road		
Balaji Cheruvu Centre	5	
Balaji Cheruvu Centre Towards Devalayam Street		
Balaji Cheruvu Centre Towards Masjid Street		
Balaji Cheruvu Centre Towards GH Road		
Balaji Cheruvu Centre Towards Pindalcheruvu Road		
II Town PS Centre	5	
II Town PS Side Road		
II Town PS Towards Bhanugudi Road		
II Town PS Side Road Towards Main Road		
II Town PS Side Road Towards Main Road		

Anand Theatre Centre	5	
Anand Theatre Centre		
Anand Theatre Centre		
Anand Theatre Centre		
Anand Theatre Centre		
Bhanugudi Centre	5	
Bhanugudi Centre		
Bhanugudi Centre		
Bhanugudi Centre		
Bhanugudi Centre		
DSP Office	4	
DSP Office		
DSP Office		
DSP Office		
Nagamallithota Junction	4	
Nagamallithota Junction Towards SP Office		
Nagamallithota Junction Towards SP Office		
Nagamallithota Junction Towards SP Office		
Sarpavaram Junction	5	
Sarpavaram Junction		
Sarpavaram Junction		
Sarpavaram Junction		
Sarpavaram Junction		
Atchampeta Junction	6	
Atchampeta Junction		
Atchampeta Junction		
Atchampeta Junction		
Atchampeta Junction		
Atchampeta Junction		
Indrapalem Bridge Junction	5	
Indrapalem Bridge Junction Towards New Bridge		
Indrapalem Bridge Junction Towards Indrapalem Bridge		
Indrapalem Bridge Junction Towards Gandhi Nagar Road		
Indrapalem Bridge Junction Towards Zilla Parishad Junction		
Light House Junction	5	
Light House Junction Towards NFCL Road		
Light House Junction Towards Port Road		
Light House Junction Towards Uppada Road		

Light House Junction Towards Achuthapuram Road		
RTC Bus Stand	4	
RTC Complex Towards RTC In L		
RTC Complex Towards RTC In R		
RTC Complex Towards RTC Exit		
Kokila Centre Junction	4	
Kokila Centre Junction Towards Kokila Road		
Kokila Centre Junction Towards Bridge		
Kokila Centre Junction Peta		
Railway Station VIP Gate	5	
Railway Station Gate 1 Enterence		
Raiway Station Towards Raithu Bajar		
Railway Station 3		
Raiway Station Towards Gate 2 Enterence		
Zilla Parishad Centre PTZ	5	
Zilla Parishad Centre Towards New Bridge		
Zilla Parishad Centre Towards GH Road		
Zilla Parishad Centre DSP Office		
Zilla Parishad Centre Towards Collectorate		
ADB Road Fly Over Junction	4	
ADB Road Towards Indrapalem Road		
ADB Road Towards Achuthapuram Road		
ADB Road Towards Samarlakota Road		
JNTU Junction	4	
JNTU Junction		
JNTU Junction		
JNTU Junction		
Prathapnagar Towards Gandhi Nagar Raod	3	
Prathapnagar Towards Samarlakota Road		
Prathapnagar Towards Indrirapalem Bridge Road		
Govt.General Hospital Centre Towards PR College Road	3	
Govt.General Hospital Centre Towards Balacheruvu Road		
Govt.General Hospital Centre Towards Zillparishad Road		
Kalpana Center Towards Dairyfarm Center Bridge	4	
Kalpana Center Towards		
Kalpana Center Towards		

Kalpana Center Towards		
Karanamgari junction Towards Nagamalli Thota Road	3	
Karanamgari junction Towards Achuthapuram Gate Road		
Karanamgari junction Towards Bhanugu Road		
Collectorate Junction	**2**	192.168.210.130
Collectorate Junction Gate		192.168.210.131
Dairy Farm Center	**5**	192.168.210.132
Dairy Farm Center Towards Sanjeevnagar		192.168.210.133
Dairy Farm Center Towards Beach Road		192.168.210.134
Dairy Farm Center Towards Gurralagunta		192.168.210.135
Dairy Farm Center Towards Kalpana Center Road		192.168.210.136
3 Lights Junction	**4**	192.168.210.137
3Lights Junction		192.168.210.138
3Lights Junction		192.168.210.139
3Lights Junction		192.168.210.140
Total	123	

Annexure III - Solution Requirements & Locations

Indicative List and Exact number after due Survey and Assessment

Sl No	Solution Requirement	# of Devices
1	CCTV Cameras (PTZ)	150
2	CCTV Camera (Fixed Box)	200
3	Automatic Number Plate Recognition	50
4	Red Light Violation Detection	50
5	Public Address Systems	20
6	Variable Messaging Display Systems	30
7	Thermal Cameras	20
8	Face Recognition Systems	20

Annexure IV - Indicative Length of City Network Bone

Details on Kakinada Network Bone

Indicative List and Exact number after due Survey and Assessment

Sl No	Area Within Kakinada	Length of network to be laid
1	31.52 Sq. KMs	250 KMs

Annexure V - Proposed Locations of Zonal Aggregation Points

Sl No	Locations	Approximate Coordinates
1	Six Zonal Aggregation Points connecting Ward (50) access backbone	To be assessed during survey

This would be an indicative list of locations, SI is expected to carry out an independent assessment and propose for the same for different locations for housing the zone level aggregation points. Ward Aggregation points are expected to be identified by SI

Annexure VI- Indicative list of Environmental Sensors Installation Locations

Sl #	Indicative List
1	Sarpavaram Junction
2	Bhanugudi Centre
3	Masjid Centre
4	Jaganniakpur Bridge
5	Municipal Office

Annexure VII - Locations for Smart Lighting

Sl No.	Locations for Smart Lighting
1	Existing - 12,500
2	Requirement - 20,000

Annexure VIII - ICT based Solid Waste Management

Sl No	Component	
1	Collection Points	200
2	Bins to be RFID tagged	300
3	Fleet Size	75

Exact Requirements are to be assessed during survey

Annexure IX - Locations of Parking Lots

Sl No	Area/Location	Parking Lots	Possession	Space for Four Wheeler	Space for two Wheeler
1	City	100	Municipality	1000	5000

The above number is indicative and exact assessment is required to be during survey

Annexure X – City Bus Services is not relevant for Kakinada City

Annexure- XI: Standards and Guidelines

Contents

Annex-A (BioMetrics Standards)

BioMetrics Standards

The Indian Government proposes to use biometric data for identification and verification of individuals in e-Governance applications. The biometric data includes fingerprint image, minutiae, face image and iris data.

The Indian e-Governance applications will have both biometric identification and verification phases, to ensure there is no duplication of identity and to verify the identity of a person for access to the services of the application.

1) Face Image Data Standard

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

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

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

Standard	Description
ISO /IEC 19794-5:2005(E)	This standard includes capture and storage specifications of face images for human visual inspection and verification of the individuals in Indian E-Governance applications. It specifies a format to store face image data within a biometric data record compliant to the Common Biometric Exchange Formats Framework (CBEFF), given in ISO 19785-1. It also includes best practices recommended for implementation of the specifications in different categories of e-Governance applications. The scope of this standard includes: 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.

2) Fingerprint Image and Minutiae Data Standard

Fingerprint is an important and unique biometric characteristic of an individual. There are many vendors selling finger print devices for acquisition of the data in different ways. Also various algorithms are available for fingerprint features extraction and matching.
It is necessary that these vendors follow fingerprint standards and best practices to ensure interoperability of devices and algorithms to avoid vendor lock-in, and also ensure long term storage of data with technology independence.

Usually, the fingerprint image data captured during enrolment is stored / transmitted for 1:1 (verification) and 1: N (identification) in an e-Governance application life cycle.

The matching of the fingerprints is done by extracting the minutiae of fingerprint data already stored in the enrolment stage, with the minutiae of data captured at the time of verification / identification. This process may even require transmission of fingerprint image data / minutiae data among various e-Governance applications by following the best practices.

Standard	Description
ISO/IEC 19794-4:2005(E)	This standard deals with usage of fingerprint image data and minutiae data for identification and verification of an individual. To ensure interoperability among vendors, it is required that these images be stored in a format compliant with the international standard ISO 19794-4, within the overall Common Biometric Exchange Formats Framework (CBEFF) as per ISO 19785-1. The Government of India would adopt ISO/IEC 19794-4:2005(E) as Fingerprint Image standard, and ISO 19794-2:2005(E) as Minutiae data format standard. The current version of Fingerprint image data standard has been tailored from the ISO 19794-4:2005(E) standard to meet specific needs of e-Governance applications in Indian context. It also includes best practices recommended for implementation of the specifications in different categories of e-Governance applications. This standard specifies fingerprint image specifications in different stages like acquisition for enrolment / verification / identification, storage and transmission. It also includes minutiae template specifications and best practices for implementation of the standard specifications in different categories of e-Governance applications based upon the volume of data, and verification/ accuracy requirements. The current version of the standard is applicable to all civilian e-governance applications as the present version does not include specifications for latent fingerprint data required by certain law enforcement applications.

3) Iris Image Data Standard

In the recent years, Iris recognition has emerged as an important and powerful Biometric characteristic. The Indian Government anticipates that, iris biometric would be deployed for identification and verification in e-Governance applications where identity management is a major issue.
In order to capture the Iris image, special devices are available in the market providing different formats for image acquisition and storage. Also many algorithms have been developed by vendors to extract the features of iris images to decide on a match during

verification / identification stage. To ensure interoperability among the e-Governance applications requiring iris recognition, it is necessary to standardize iris specifications including the storage and transmission formats.

Thus, to allow the application developer maximum flexibility in usage of algorithms and devices from different vendors and to address interoperability requirements, the iris image must be captured and stored as per standard specifications included in this document.

This Standard would be applicable to all e-Governance applications in India as per the Government's Policy on Open Standards.

There are two types of interchange formats to represent the Iris image data. The first is a rectilinear (rectangular or Cartesian) image storage format that specifies raw, uncompressed or compressed intensity values. The second format is based on polar image specification with specific pre processing and segmentation steps, producing a compact data structure containing only Iris information.

The Indian e-Governance applications will deal with Iris image data during multiple stages. Some of these stages are given below:

a. Image acquisition, its processing and its storage in the Enrolment stage
b. Image acquisition and storage for off line / on line verification of Iris image data in 1:1 matching stage
c. Image acquisition and storage for the purpose of identification in 1:N matching stage
d. Transmission of Iris image data to other e-Governance applications
e. Extraction of features of Iris images (enrolment or recognition stage), their storage, and matching (Not covered in the present version of the standard).

The interchange format type of the Iris images that is defined in this standard is for **rectilinear images only**.

If the image is collected by a camera that captures only one eye at a time and is stored using a rectilinear coordinate system no specific pre-processing is required. Cameras that capture images of botheyes simultaneously may use the following processing steps to calculate the rotation angle of the Iris images.

Standard	Description
ISO/IEC 19794-4:2005(E)	The Government of India would broadly adopt ISO 19794-6:2005(E) Iris Image Data Standard, by tailoring the standard specifications to meet specific needs of civilian e-Governance applications in Indian context and as per the GoI Policy on Open Standards. This Standard specifies Iris image data specifications, acquisition, storage and transmission formats. It also includes best practices for implementation of the Standard specifications in different categories of e-Governance applications, based on the volume of data and verification/ accuracy requirements. This version of the Standard does not include features extraction & matching specifications.

Reference Standards:

1. GoI Face Image data standard version 1.0 published in November, 2010
2. GoI Fingerprint Image data Standard version 1.0 published in November, 2010
3. GoI Iris Image Data Standard Version 0.4, document published in March, 2011

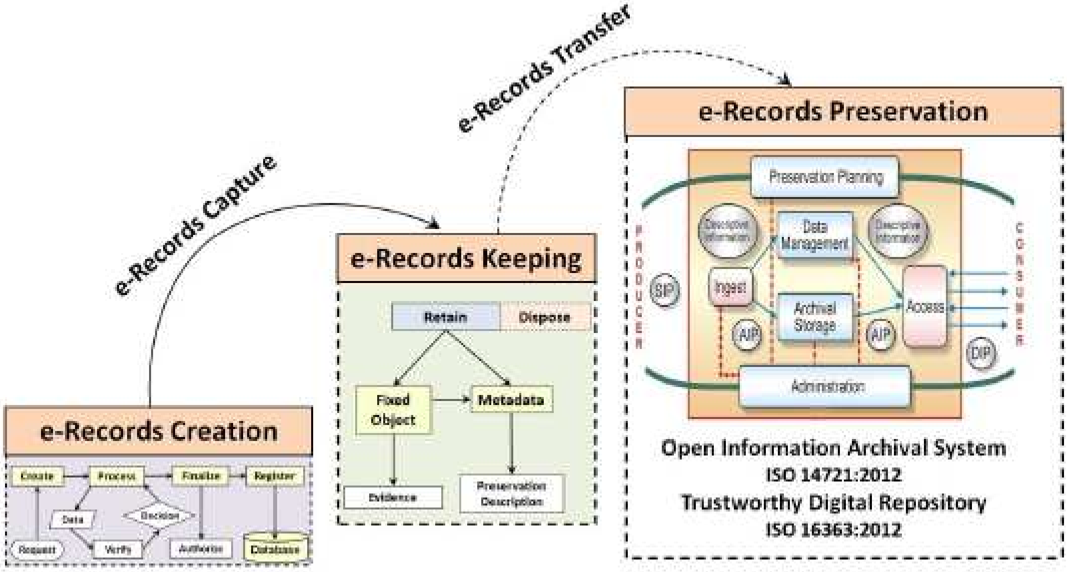
Annex-B (Digital Preservation Standards)

The **e-Governance Standard for Preservation Information Documentation (eGOV-PID) of Electronic Records (eGOV-PID)** provides a standardized metadata dictionary and schema for describing the "preservation metadata" of an electronic record. This standard proposes to capture most of the preservation information (metadata) automatically after the final e-record is created by the e-Government system. Such preservation information documentation is necessary only for those e-records that need to be retained for long durations (e.g. 10 years, 25 years, 50 years and beyond) and the e-records that need to be preserved permanently.

The implementation of this standard helps in producing the valid input i.e. Submission Information Package (SIP) for archival and preservation purpose as per the requirements specified in the ISO 14721 Open Archival Information Systems (OAIS) Reference Model.

The eGOV-PID allows to capture the preservation metadata in terms of cataloguing information, enclosure information, provenance information, fixity information, representation information, digital signature information and access rights information.

The core concepts of ‘preservability’ are based on the requirements specified in IT ACT, ISO/TR 15489-1 and 2 Information Documentation - Records Management and ISO 14721 Open Archival Information Systems (OAIS) Reference Model. It introduces 5 distinct steps of e-record management i.e. e-record creation, e-record capturing, e-record keeping, e-record transfer to designated trusted digital repository and e-record preservation which need to be adopted in all e-Governance projects.



Standard	Description
ISO 15836:2009	Information and documentation - The Dublin Core metadata elements
ISO/TR 15489-1 and 2	Information and Documentation - Records Management: 2001
ISO 14721:2012	Open Archival Information Systems (OAIS) Reference Model
ISO/DIS 16363: 2012	Audit & Certification of Trustworthy Digital Repositories
METS, Library of Congress, 2010	Metadata Encoding and Transmission Standard (METS) -
InterPARES 2	International Research on Permanent Authentic Records - A Framework of Principles for the Development of Policies, Strategies and Standards for the Long-term Preservation of Digital Records, 2008
ISO 19005-1:2005 Use of PDF 1.4 (PDF/A-1b) with Level B	Capture of e-records in PDF for Archival (PDFA) format - PDF/A-1a is based on the PDF Reference Version 1.4 from Adobe Systems Inc. (implemented in Adobe Acrobat 5 and latest versions) and is defined by ISO 19005-1:2005. Conformance is recommended for archival of reformatted digital documents due to following reasons: o PDF/A-1b preserves the visual appearance of the document o Digitized documents in image format can be composited as PDF/A-1b **PDF/A for e-governance applications** o Apache FOP 1.1 library can be used in the application logic for dynamically publishing the e-records in PDF/A format. **PDF/A for document creation** o Libre Office 4.0 supports the exporting of a document in PDF/A format. o MS Office 2007 onwards the support for “save as” PDF/A is available. o Adobe Acrobat Professional can be used for converting the PDF documents to PDF/A format.
ISO 19005-2:2011 Use of ISO 32000-1 (PDF/A-2)	Recommended for preservation of documents requiring the advanced features supported in it. PDF/A-2a is based on ISO 32000-1 – PDF 1.7 and is defined by ISO 19005-2:2011. Its features are as under: o Support for JPEG2000 image compression o Support for transparency effects and layers o Embedding of OpenType fonts o Provisions for digital signatures in accordance with the PDF Advanced Electronic Signatures – PAdES standard o Possibility to embed PDF/A files in PDF/A-2 for archiving of sets of documents as individual documents in a single file PDF/A-2 does not replace the PDF/A-1 standard but it co-exists alongside with an extended set of features. PDF/A-1a and PDF/A-1b compliance are minimum essential for e-government records as recommended in the IFEG technical standard of DeitY.

Standard	Description
JPEG2000 (ISO/IEC 15444-1:2004) and PNG (ISO/IEC 15948:2004)	Image file formats - which support lossless compression are recommended as raster image file formats for e-governance applications as specified in Technical Standards for Interoperability Framework for e-Governance (IFEG) in India, published in 2012 by e-Gov Standards Division, DeitY.
ISO/IEC 27002: 2005	Code of practices for information security management for ensuring the security of the e-records archived on digital storage.

Annex-C (Localisation and Language Technology Standard)

1. Character Encoding Standard for Indian Languages

The lack of availability of information in the locally understandable language is the main reason for the slow progress in the Information and Communication Technology (ICT) sector. In today's age, access to ICT plays a major role in the overall development of a country, it has become a challenge to bridge the digital divide caused by the language barrier.

Standardization is one of the baselines to be followed in localization. Standardization means to follow certain universally accepted standards, so that the developers from any part of the globe could interact through the application. Standardization becomes applicable in almost everything specific to the language – for instance, a standard glossary of terms for translation, a standard keyboard layout for input system, a standard collation sequence order for sorting, a standard font etc.

Character Encoding standard for all constitutionally recognized Indian Languages should be such that it facilitates global data interchange.

ISCII is the National Standard and Unicode is the global character encoding standard. The average data packet size is less for representation of any Indian languages using ISCII. However, being limited code space, coexistence of multiple languages within the same code page is not possible in ISCII. The migration from ISCII to Unicode has become imperative due to the following reasons:

All major operating systems, browsers, editors, word processors and other applications & tools are supporting Unicode.

- It is possible to use Indian languages and scripts in the Unicode environment, which will resolve the compatibility issue.
- The documents created using Unicode may be searched very easily on the web.
- As Unicode is widely recognized all over the world and also supporting Indian languages, it will ease Localization applications including e-Governance application for all the constitutionally recognized Indian languages.
- Since Indian languages are also used in the other part of the world, it is possible to have Global data exchange.

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

Specification Area	Standard Name	Owner	Nature of the Standard	Nature of Recommend Actions
Character Encoding for Indian Languages	Unicode 5.1.0 and its future upgradation as reported by Unicode consortium from time to time.	Unicode Consortium, Inc.	Matured	Mandatory

Character: Character is the smallest component of any written language that has semantic value.

ISCII: Indian Script Code for Information Interchange (ISCII - IS 13194:1991) is the character-encoding standard approved by Bureau of Indian Standards (BIS). ISCII is an 8 bit-encoding scheme, catering to 128 code spaces for representation of Indian languages.

Nine Indian scripts are included in ASCII standard to represent 10 Indian languages i.e. Assamese, Bengali, Devnagari, Gujarati, Gurmukhi, Kannada, Malayalam, Oriya, Tamil and Telugu.

Unicode: Unicode is a 16-bit character-encoding standard. All the major written scripts of the world are included in the Unicode Standard. The first version of Unicode was published in year 1991.

Unicode vis-à-vis ISO10646

Unicode is a 16 bit Character Encoding standard. All the major written scripts are included in the Unicode Standard. Indian scripts are also included in the standard. There are 22 constitutionally recognized Indian Languages, written in 12 different scripts. ISO/IEC 10646 is the character-encoding scheme evolved by the International Organization for Standardization (ISO) in 1990.

In 1991, the ISO Working Group responsible for ISO/IEC 10646 (JTC 1/SC 2/WG 2) and the Unicode Consortium decided to create universal standard for coding multilingual text. Since then, the ISO 10646 Working Group (SC 2/WG 2) and the Unicode Consortium are working together closely to extend the standard and to keep their respective versions synchronized.

In addition to the code tables as per ISO/IEC 10646, the Unicode Standard also provides an extensive set of character specifications, character data, algorithms and substantial technical material, which is useful for developers and implementers.

2. Font Standard for Indian Languages

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

True Type Fonts (TTF) was used in various applications earlier by various vendors. TTF had no encoding standard due to which vendors and developers had their own encoding schemes, thereby jeopardizing data portability. ISO/IEC 14496-OFF (Open Font Format) on the other hand is based on a single International Standard and complies with UNICODE for data storage. This ensures data portability across various applications and platforms. Open type font is a smart font which has built- in script composition logic.

Most often it has been observed that the use of proprietary fonts of different standards in Government Offices, which are not compatible with each other, is causing serious problems in information exchange amongst offices. By using Unicode compliant ISO/IEC 14496-OFF (Open Font Format) for font standard, the problem relating to the exchange of documents/files is completely solved.

Open standard under the International Organization for Standardization (ISO) within the MPEG group, which had previously adopted Open Type by reference, now adopted the new standard with appropriate language changes for ISO, and is called the "ISO/IEC 14496-OFF (Open Font Format)" for which formal approval reached in March 2007 as ISO Standard ISO/IEC 14496-OFF (Open Font Format) and it is a free, publicly available standard.

ISO/IEC 14496-OFF (Open Font Format) for font standard would be the standard for Indian Languages in e-Governance Applications. **ISO/IEC 14496-OFF (Open Font Format) for font standard is mandatory for all 22 constitutionally recognized languages.**

TTF (True Type Font)

A Font Format developed by Apple and licensed to True type, is the native Operating System Font Format for Windows and Mac operating systems.

ISO/IEC 14496-OFF (Open Font Format)

OFF fonts allow the handling of large glyph sets using Unicode encoding. Such encoding allows broad international support for typographic glyph variants.

OFF fonts may contain digital signatures, which enable operating systems and browsing applications to identify the source and integrity of font files, (including the embedded font files obtained in web documents), before using them. Also, font developers can encode embedding restrictions in OFF fonts which cannot be altered in a font signed by the developer.

Annex-D (Metadata and Data Standards)

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

Data Standards may be defined as the agreed upon terms for defining and sharing data. Data Standards promote the consistent recording of information and are fundamental to the efficient exchange of information. They provide the rules for structuring information, so that the data entered into a system can be reliably read, sorted, indexed, retrieved, communicated between systems, and shared. They help protect the long-term value of data.

Once the data standards are in place, there is a need to manage data, information, and knowledge. Metadata of standardized data elements can be used for this purpose.

Metadata is structured information that describes, explains, locates or otherwise makes it easier to retrieve, use or manage an information resource. Metadata is often called data about data or information about information. A metadata is a matter of context or perspective -what is metadata to one person or application can be data to another person or application.

In other words, Metadata facilitates the user by providing access to the raw data through which the user can have an understanding of the actual data. Hence, Metadata is an abstraction layer that masks the underlying technologies, making the data access friendlier to the user.

Data and Metadata Standards provide a way for information resources in electronic form to communicate their existence and their nature to other electronic applications (e.g. via HTML or XML) or search tools and to permit exchange of information between applications.

The present document “Data and Metadata Standards- Demographic” focuses on Person Identification and Land Region codifications. It includes the following:

a) **Mechanism for allocation of reference no**. to the identified Generic data elements, and their grouping.

b) **Generic data elements** specifications like:

- Generic data elements, common across all Domain applications
- Generic data elements for Person identification
- Generic data elements for Land Region Codification
- Data elements to describe Address of a Premises, where a Person resides

c) **Specifications of Code Directories like:**

- Ownership with rights to update
- Identification of attributes of the Code directories
- Standardization of values in the Code directories

d) Metadata of Generic Data Elements

- Identification of Metadata Qualifiers
- Metadata of the data elements

e) Illustration of data elements to describe:

- Person identification
- Address of a premises

This Standard would be applicable to all e-Governance applications in India as per the Government’s Policy on Open Standards (refer http://egovstandards.gov.in/policy/policy-onopen-standards-for-e-governance/)

Reference Standards:

1. ISO Standard 1000:1992 for SI Units
2. MNIC Coding for Person Identification
3. ISO 693-3 for International language codes

4. RGI’s coding schemes for Languages
5. Top level document provided by Working Group on Metadata and Data Standards
6. EGIF (e- Government Interoperability Framework) Standard of U.K.
7. uidai.gov.in/UID_PDF/Working_Papers/A_UID_Numbering_Scheme.pdf
8. http:// www.dolr.nic.in for conversion table of units as used by Department of Land Records
9. GoI Policy on open standards version 1.0 released in November, 2010
10. UID DDSVP Committee report, Version 1.0, Dec 09, 2009
11. ANSI92 Standard

Annex-E (Mobile Governance)

Framework for Mobile Governance (m-Governance)

Mobile Governance (m-Governance) is a strategy and its implementation to leverage available wireless and new media technology platforms, mobile phone devices and applications for delivery of public information and services to citizens and businesses.

The m-Governance framework of Government of India aims to utilize the massive reach of mobile phones and harness the potential of mobile applications to enable easy and round the-clock access to public services, especially in the rural areas**.** The framework aims to create unique infrastructure as well as application development ecosystem for m-Governance in the country.

In cognizance of the vast **mobile phone subscriber base, peaked to more than 1 billion users in the country**, the Government has decided to also provision for access of public services through mobile devices, thereby establishing mobile Governance (m-Governance) as a compelling new paradigm.

Government of India will progressively adopt and deploy m-Governance in a time-bound manner to ensure inclusive delivery of public services to both the urban and rural populace in the country in accordance with this framework.

The following are the main measures laid down:

i. Web sites of all Government Departments and Agencies shall be made mobile compliant, using the "**One Web"** approach.

ii. **Open standards** shall be adopted for mobile applications for ensuring the interoperability of applications across various operating systems and devices as per the Government Policy on Open Standards for e-Governance.

iii. **Uniform/ single pre-designated numbers** (long and short codes) shall be used for mobile-based services to ensure convenience.

iv. All Government Departments and Agencies shall develop and deploy mobile applications for providing all their public services through mobile devices to extent feasible on the mobile platform. They shall also specify the service levels for such services.

The success of the proposed initiative on m-Governance will greatly depend upon the ability of the Government Departments and Agencies to provide frequently needed public services to the citizens, create infrastructure for anytime anywhere mobile-based services, adopt appropriate open standards, develop suitable technology platforms, make the cost of services affordable, and create awareness, especially for people in underserved areas.

To ensure the adoption and implementation of the framework in a time-bound manner, following actions will be taken:

1. **Creation of Mobile Services Delivery Gateway (MSDG)**

MSDG is the core infrastructure for enabling the availability of public services through mobile devices. This will be developed and maintained by an appropriate agency within DIT. MSDG is proposed to be used as a shared infrastructure by the Central and State Government Departments and Agencies at nominal costs for delivering public services through mobile devices.

Various channels, such as voice, text (e-mail and SMS), GPRS, USSD, SIM Toolkit (STK), Cell Broadcast (CBC), and multimedia (MMS) will be incorporated to ensure that all users are able to access and use the mobile based services. The various delivery channels are expected to entail innovative ways of providing existing services as well as development of new services.

To ensure successful implementation of the platform with requisite levels of security and redundancy, following actions will be taken:

a) **End User Interface:** End-user devices include landline phones, mobile phones, smart phones, personal digital assistants (PDAs), tablets, and laptops with wireless infrastructure. Mobile applications developed shall take into consideration appropriately the wireless-device interface issues, such as bandwidth limitations, micro-browser and micro-screen restrictions, memory and storage capacities, usability, etc.

b) **Content for Mobile Services:** Due to lower-bandwidth and smaller-screen characteristics of mobile devices, successful development and deployment of m-Governance will require development of separate mobile-ready content. Similarly, to meet the needs of all the potential users, the applications will need to be developed in the relevant local languages for the various channels of delivery. Open standards and open source software, to the extent possible, will be used to ensure interoperability and affordability of the content and applications developed.

c) Mobile Applications (Apps) Store: A mobile applications (m-apps) store will be created to facilitate the process of development and deployment of suitable applications for delivery of public services through mobile devices. The m-apps store shall be integrated with the MSDG and it shall use the MSDG infrastructure for deployment of such applications. It is proposed that the store will be based upon service oriented architecture and cloud based technologies using open standards as far as practicable. The open platform will be developed and deployed in conjunction with the MSDG for making the additional value added services available to the users irrespective of the device or network operator used by them

d) Application Programming Interfaces (APIs) for Value-Added Services (VAS) providers: MSDG shall offer suitable APIs to VAS providers with appropriate terms and conditions to ensure interoperability and compliance with standards for development of applications for delivery of public services.

e) **Mobile-Based Electronic Authentication of Users**: For electronic authentication of users for mobile-based public services, MSDG shall incorporate suitable mechanisms including Aadhaar-based authentication. This will also help in ensuring appropriate privacy and confidentiality of data and transactions.

f) **Payment Gateway**: MSDG shall also incorporate an integrated mobile payment gateway to enable users to pay for the public services electronically.

g) **Participation of Departments**: The Government Departments and Agencies both at the Central and State levels will be encouraged to offer their mobile-based public services through the MSDG to avoid duplication of infrastructure.

2. Creation of Mobile Governance Innovation Fund

Department of Information Technology (DIT) shall create a Mobile Governance Innovation Fund to support the development of suitable applications by Government Departments and Agencies and also by third-party developers including start-ups. The fund shall be created and managed by DIT for a minimum period of 3 years. The objective of this fund will be to accelerate the development and deployment of the mobile applications across the entire spectrum of public services.

3. Creation of Knowledge Portal and Knowledge Management Framework on Mobile Governance

DIT shall develop and deploy a state-of-the-art knowledge portal and knowledge management framework that acts as a platform for awareness generation and dissemination for various Central Government Ministries and the State Governments. This will enhance the absorptive as well as the service provision capabilities of various stakeholders in m-Governance. Since m-Governance is in its nascent stage both in India and globally, the knowledge portal will act as a reference and guide for Government Departments and Agencies in India.

4. Creation of Facilitating Mechanism

An appropriate facilitating mechanism will be created to ensure compliance with the standards for mobile applications and ensure seamless interoperability of services and implementation of short and long codes for public services across multiple service providers. The proposed mechanism shall be established and managed by the Department of Information Technology, Government of India.

Guidelines for Delivery Channels for Provision of Public Services through Mobile Devices

The Objective is to provide:

a. **Guidelines to deliver public services round-the-clock to the users using m-Governance**

b. **Guidelines to develop standard based mobile solutions**

c. **Guidelines to integrate the mobile applications with the common e-Governance infrastructure**

As part of the initiative a shared technical infrastructure **Mobile Services Delivery Gateway (MOBILE SEVA)** has been created to enable integration of mobile applications with the common e-Governance infrastructure and delivery of public services to the users.

The objective of creating the MOBILE SEVA is to put in place government-wide shared infrastructure and services to enable rapid development, mainstreaming and deployment of m-Governance services. It will enhance interoperability across various public services as well as reduce the total cost of operation of m-Governance services by providing a common pool of resources aggregating the demand for communication and e-Governance services, and act as a platform for various Government Departments and Agencies to test, rapidly deploy, and easily maintain m-Governance services across the country.

MSDP (Mobile e-governance Services Delivery Platform) provides an integrated platform for delivery of government services to citizen over mobile devices using Mobile Service Delivery Gateway (MSDG), SMS Gateway, m-App Store, m-Payment Services, Location Based Services (LBS), Unstructured Supplementary Services Data (USSD), Unstructured Supplementary Service Notify (USSN), Unstructured Supplementary Service Request (USSR), MMS, Cell Broadcasting Service (CBS), SIM Toolkit (STK), IVRS etc.

MSDG is a messaging middleware to facilitate e-Governance services delivery based on e-Governance Standard protocols which are IIP (Interoperability Interface Protocol), IIS (Interoperability Interface Specifications), IGIS (Inter-Gateway Interconnect Specifications) and Gateway Common Services Specifications (GCSS).

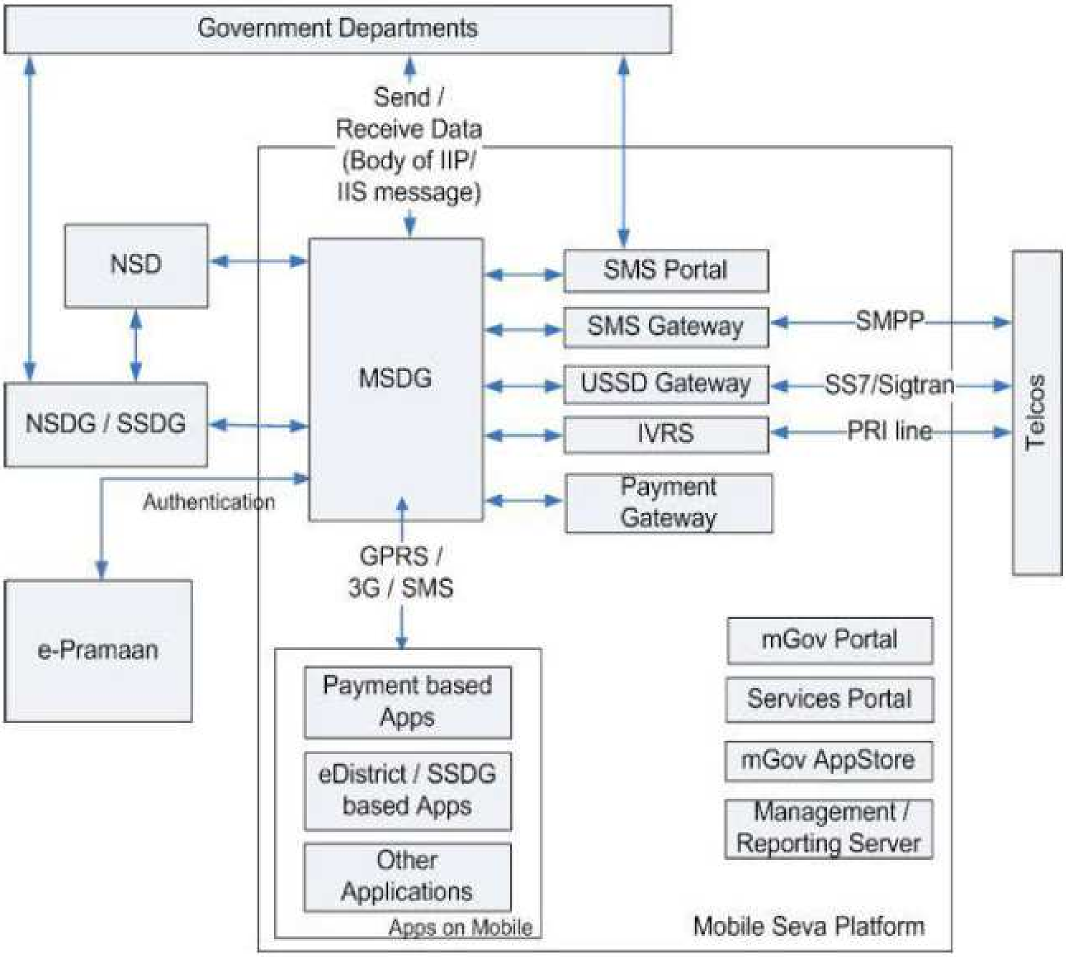


Figure 1: Mobile e-governance Services Delivery Platform (MSDP)

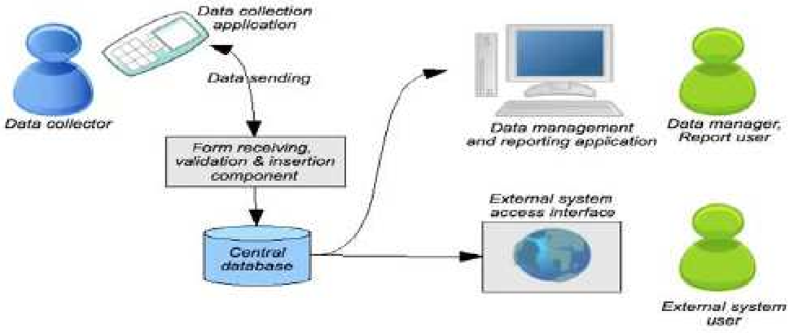
Mobile Application (m-Apps)

Mobile application software is applications software developed for handheld devices, such as mobile

phones, tablets etc. These applications can be pre-installed on phones during manufacture or downloaded by users from various mobile software distribution platforms, or delivered as web applications using server-side or client-side processing (e.g. JavaScript) to provide an application like experience within a Web browser.

1. **Mobile Application Dependency on Handset and O/S**
   Mobile Application software developers also have to consider a lengthy array of screen sizes, hardware specifications and configurations because of intense competition in mobile software and changes within each of the platforms.

2. **Data Collection: m-forms**
   Mobile Application can also make use of the various forms for data collection. Many data collection systems are built from existing commercial or open source components, or even come packaged as an end-to-end solution. The components of data collection relate to each other as shown below:


Data collection application
Data sending
Data collector
Form receiving, validation & insertion component
Central database
Data management and reporting application
Data manager, Report user
External system access interface
External system user

The data collection may be done by various methods. Following are the most common types of data collection client applications which may be used:

1. **Fixed format SMS based Forms:** The 'client application' in this case is the phone's built-in SMS functionality. The user writes and sends SMS in a predefined format, representing answers to successive questions.

2. **Java Micro Edition Platform (J2ME) Application based Forms:** A J2ME application is written in the Java programming language, and loaded onto the phone over Bluetooth or by downloading the application from the Internet. To use the client application, the data collector navigates through questions in an application on the phone, which collects the answers and submits the completed form to a server.

3. **Mobile Operating System based Forms:** Mobile Operating Systems such as Android, Windows Mobile can also be used for developing native platform-dependent applications which can have various forms for data collection.

4. **Web-based Forms:** The 'client application' for web-based forms is the phone's web browser. The user browses to a website, where the form is published in an optimized format for mobile browsers.

5. **Voice-based based Forms:** The user dials a number and then chooses from options on a menu, useful when there are low levels of literacy among data collectors, or when a system is needed that caters for both landline and mobile phones.

6. **Wireless Internet Gateway (WIG) based Forms:** WIG uses a programming language (Wireless Markup Language, or WML) that is internal to almost all SIM cards. The menu definition is easy to write, but the size limit is 1MB, making it difficult to support long menus or multiple languages.

7. **Unstructured Supplementary Service Data (USSD) based Forms:** This is a real-time question-response service, where the user initiates a session and is then able to interact with the remote server by selecting numeric menu options. The phone needs to be continuously connected during the session, which needs a good, consistent signal.

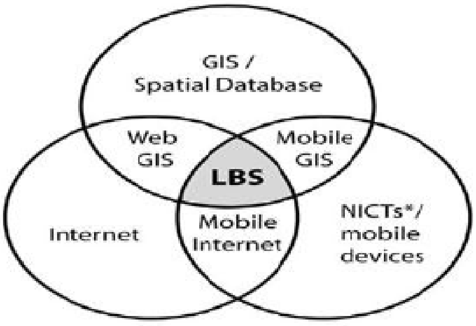
Once data has been captured on the phone, the completed form generally needs to be submitted to a central back-end server.

Other Mobile Technologies

1. Location Based Services (LBS)

Location-based services (LBS) denote services offered to mobile users according to their geographic location. LBS give the possibility of a two way communication and interaction. Therefore the user tells the service provider his actual context like the kind of information he needs, his preferences and his position. This helps the provider of such location services to deliver information tailored to the user needs. LBS enable to retrieve and share information related to their current position. For e.g. Google Latitude.

It works as an intersection of the following features in a system:



***NICT – New Information and Telecommunication technologies**

Geographical Information System (GIS) is a hardware, software and procedures designed to support the capture, management, manipulation, analysis, modelling and display of spatially referenced data for solving complex planning and management problems.

Internet is used to utilize the database dynamically so as to provide the appropriate service.
Mobile Devices as an end- device to execute the service.

2. Cell Broadcast Centre

Cell Broadcast is a mobile technology which allows text messages to be broadcasted to all mobile handsets and similar devices within a designated geographical area.
It is a one-to-many geographically focused service, in contrast to SMS which is a one-to-one or one-to-few service. It is usually used for providing location-based services, especially emergency services, as it utilizes minimum network resources for message broadcast and provides instantaneous delivery to all subscribers in a geographic area.
A Cell Broadcast message is an unconfirmed push service, meaning that the originator of the message does not know who has received the message, allowing for services based on anonymity. Mobile telephone user manuals describe how the user can switch the receiving of Cell Broadcast messages on or off.

Also known as Short message service-Cell Broadcast (SMS-CB), CB messaging is a mobile technology feature defined by the ETSI's GSM committee and is part of the GSM standard. It is also supported by UMTS, as defined by 3GPP.

a) Localization

Given that only a miniscule segment population in India can read and write English, it is important to deploy local/ regional languages to ensure all-round success of m-Governance initiatives. For detailed guidelines please refer to the Mobile Localization Guidelines.

b) Indian Language SMS

Currently, Indian language SMS services are offered by some operators but unlike the English SMS service, the language service is not necessarily interoperable across networks and cannot be availed on all types of handsets. The lack of a standard for Indian SMS comes in the way of providing scalable, interoperable and affordable SMS services in Indian languages.

To realise the goal of interoperable and affordable Indian language SMS, the following are the priority areas:

i. **Text entry standards (i.e. keypad)**
ii. **Encoding standards to support all the major Indian languages**
iii. **Font support standardization for handsets to send and receive Indian language SMS**

i. Text entry methods

The two methods in vogue are:

a. **Mapping the Indian language characters on the handset keypad**
b. **Screen-assisted text inputting mechanisms available from a few OEMs and vendors**

The keypad for the English language has been standardized by ITU. Althoughefforts on supporting the Indian languages on handheld devices are on, acceptable standards are yet to be evolved. In the absence of any national standards specifying mapping of the Hindi (and other Indian Languages) alphabets to the 12-key mobile devices, the handset vendors keen on penetrating the large Indian market are using their own mappings (which can differ across vendors).

ii.Encoding standard

The Unicode standard supports the 22 major Indian languages but uses more bandwidth (2 octets for each character) and hence the maximum size of SMS that can be sent using Unicode (70 characters) would be less than half of that of an English language SMS (170 characters).

iii. Font Support

Solutions for aesthetic display of Indian language scripts on small handset screens are being worked out. Similarly, solutions are tried out for handsets already in use so that they can receive and display messages in Indian languages, even if they cannot be used to send such messages.

3. Mobile Payment (M-Payment)

Mobile payment is an alternative payment method. Instead of paying with cash, check, or credit cards, a consumer can use a mobile phone to pay for a wide range of services; after having authenticated the user using AADHAR or any other means. The basic aim of mobile payments is to enable micropayments on low-end mobile devices which support only voice and text, in addition to higher end phones which could support web-browsing or Java application capabilities.

a. Mobile banking (M-Banking or M-Banking)

M-Banking is a term used for performing balance checks, account transactions, payments, credit applications and other banking transactions through a mobile device. The earlier mobile banking services were offered over SMS, a service known as SMS banking. With the introduction of smart phones with WAP support the mobile web is also being used for M-

Banking. Latter with the advancements of web technologies such as HTML5, CSS3 and JavaScript it became feasible to launch mobile web based services to compliment native applications.

b. Immediate Mobile Payment Services (IMPS)

The Immediate Mobile Payment System (IMPS) has been developed by the National Payments Corporation of India (NPCI) to expand the scope of mobile payments to all sectors of the population. IMPS offer an instant, 24X7, interbank electronic fund transfer service through mobile phones.

An IMP provides an inter-operable infrastructure to the banks for enabling interbank real time funds transfer transactions. IMPS rides on the existing NFS Interbank ATM transaction switch infrastructure and message format making it easy for banks to adopt.

To enable the transfer of money, both the sender and the receiver of payment have to link their bank accounts with their phone numbers through their respective banks. The sender has to register for mobile banking service with her/his bank. Upon registration, the bank will provide a link to the Mobile banking software which needs to be installed in the mobile phone to enable payments.

Both the sender and the receiver will receive a Mobile Money Identifier (MMID) while the sender will also receive a Mobile PIN (MPIN) for authentication of transactions. While transacting, the sender has to input the MPIN, receiver’s mobile number and MMID, and the amount of funds to transfer.

IMPS will authenticate the sender, check the receiver’s mobile number and MMID, and transfer the funds to the receiver’s account in real-time. Both the sender and the receiver receive messages notifying them about the success or failure of the transaction.

c. Contactless cards and Mobile Phones

These cards are based upon a technology known as NFC (Near Field Communication) that allows NFC enabled cards to be ready by taping them on or by passing them by, a card reader than swiping them through or inserting into, the POS terminal. They are now being integrated into mobile phone handset for m-Payments.

NFC enabled phones are expected to become more widely available. The NFC chip inside the phone will be connected to the secure element within the SIM card, allowing information stored in an m-wallet to be accessed by the NFC card reader. Authorization for payments involves entering a PIN.

d. Airtime balance for payment

Airtime as balance for payment was realized because of the need for the unbanked majority to easily and cheaply transfer funds around the country. The facility required is the most basic of mobile phones, an account, which can be opened at any one of vendors to start transferring and receiving money.

Since the system uses either SIM toolkit or USSD technology depending on the country, the network charges are minimal to nonexistent. It has lowest entry barriers, since it works on more than 95 percent of handsets and has low transaction costs and no bank account or credit card required.

e. Mobile Wallet

A Mobile Wallet is functionality on a mobile device that can securely interact with digitized valuables thereby making payments using the mobile phone. Mobile wallet may reside on a phone or on a remote network / secure server. It is controlled by the user of the wallet.

Using a mobile wallet to make a payment is incredibly simple. When it is time to pay, the user turns on his or her phone’s screen (if the screen is off, when the phone is dormant for instance, the NFC chip will not work), opens the wallet application, enters their pin number, and passes the phone within a few inches of the contactless payment symbol. The payment transaction is then processed just like a conventional card transaction. In addition, relevant offers, discounts, and coupons can be passed from the wallet along with the payment in that same tap of the phone.

4. SIM Application Toolkit

The SIM Application Toolkit is a standard set of commands, under GSM, which defines how the card should interact with the outside world and extends the communication protocol between the card and the handset. It is designed as a client server application.

With SIM Application Toolkit, the card has a proactive role in the handset, i.e., the SIM initiates commands independently of the handset and the network. This enables the SIM to build up an interactive exchange between a network application and the end user and access, or control access to, the network. The SIM also gives commands to the handset such as displaying menus and/or asking for user input.

Annexure-F (GIGW)

Guidelines for Indian Government Websites

India, the largest democracy in the world, is set to emerge as an ICT Superpower in this millennium. Realizing the recognition of 'electronic governance' as an important goal by Governments world over, Indian Government has also laid a lot of emphasis on anytime, anywhere delivery of Government services. As of today, there are over five thousand Government websites in India.

Awareness about the fast changing ICT world and keenness to keep pace with the latest has ensured that almost all the State Governments in India already have their websites up and running. In fact each state has multiple websites belonging to different Departments.

However, these websites follow different Technology Standards, Design Layouts, Navigation Architecture, or, in simple terms, different look and feel as well as functionality.

The need for standardization and uniformity in websites belonging to the Government cannot be stressed enough, in today's scenario.

As a first step, it is suggested that the Indian Government websites adhere to certain common minimum standards which have been derived, in the form of guidelines discussed in this document, as prerequisites for a Government website to fulfil its primary objective of being a citizen centric source of information & service delivery. These guidelines could eventually form the basis for establishment of the desired standards.

Compliance to these guidelines will ensure a high degree of consistency and uniformity in the content coverage and presentation and further promote excellence in Indian Government Web space.

These Guidelines have been framed with an objective to make the Indian Government Websites conform to the essential pre-requisites of UUU trilogy i.e. Usable, User-Centric and Universally Accessible. They also form the basis for obtaining Website Quality Certification from STQC (Standardization Testing Quality Certification) an organization of Department of Information Technology, Government of India.

These Guidelines are based on International Standards including ISO 23026, W3C's Web Content Accessibility Guidelines, Disability Act of India as well as Information Technology Act of India.

A. Indian Government Entity

All websites and Portals belonging to the Indian Government Domain at any hierarchical level (Apex Offices, Constitutional Bodies, Ministries, Departments, Organizations, States/UTs, District Administrations, and Village Panchayats et al) must prominently display a strong Indian Identity and ownership of Indian Government.

The above objective can be achieved through the following:

1. The National Emblem of India MUST be displayed on the Homepage of the websites of Central Government Ministries/Departments. The usage of National Emblem on an Indian Government website must comply with the directives as per the 'State Emblem of India (Prohibition of improper use) Act, 2005'.

   Further, the State Governments should also display the State Emblem (or the National Emblem in case the State has adopted the National Emblem as its official State Emblem) as per the Code provided in the above Act. The Public Sector organisations and autonomous bodies should display their official logo on the Homepage of the website to re-enforce their identity.

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

3. The lineage of the Department should also be indicated at the bottom of the Homepage and all important entry pages of the website. For instance, at the bottom of the Homepage, the footer may state the lineage information, in the following manner:

   i. This Website belongs to Department of Heavy Industries, Ministry of Heavy Industries and Public Enterprises, Government of India' (for a Central Government Department).

   ii. This Website belongs to Department of Industries, State Government of Himachal Pradesh, India' (for a State Government Department).

   iii. This is the official Website of Gas Authority of India Limited (GAIL), a Public Sector Undertaking of the Government of India under the Ministry of Petroleum and Natural Gas (for a Public Sector Undertaking).

   iv. This is the official Website of the District Administration of Thanjavur, State Government of Tamil Nadu (India)' (for a District of India).

4. All subsequent pages of the website should also display the ownership information in a summarised form. Further, the searchengines often index individual pages of a website and therefore, it is important that each webpage belonging to a site displays the relevant ownership information.

5. In case of those websites which belong to Inter-Departmental initiatives involving multiple Government Departments which are difficult to list on the Homepage, the Government ownership should still be reflected clearly at the bottom of the page with detailed information provided in the 'About the Portal/Website' section.

6. The page title of the Homepage (the title which appears on the top bar of the browser) MUST be complete with the name of the country included, for instance, instead of the title being just Ministry of Health and Family Welfare, it should state, Government of India, Ministry of Health & Family Welfare.

   Alternatively, in case of a State Government Department, it should state 'Department of Health, Government of Karnataka, India '. This will not only facilitate an easy and unambiguous identification of the website but would also help in a more relevant and visible presence in the searchengine results. Further, it is important since the screen readers used by the visually impaired users first read the title of the page and in case the title is not explanatory enough, it may confuse or mislead them.

B. Government Domains

The URL or the Web Address of any Government website is also a strong indicator of its authenticity Kakinada and status as being official. In today's era with a large proliferation of websites, which resemble Government websites and fraudulently claim to provide reliable Government information and services, the role of a designated Government domain name assumes a lot of significance.

Hence, in compliance to the Government's Domain Name Policy, all Government websites MUST use 'gov.in' or 'nic.in' domain exclusively allotted and restricted to Government websites. The military institutions and organisations in India may also use 'mil.in' domain in place of or in addition to the gov.in /.nic.in domain. The above naming policy applies to all Government websites irrespective of where they are hosted.

Those Departments and Government entities that are using and have been publicising a domain name other than the above should take appropriate early action to register official government domain names and use the existing ones as ‘alias’ for a period of six months. An intermediary page with a clear message notifying the visitors about the change in the URL and then auto redirecting them to the new URL after a time gap of 10 seconds should be used.

The Domain Name Conventions, as specified in the ‘.IN Registration’ policy should be followed while registering a ‘gov.in’ Domain Name.

National Informatics Centre (NIC) is the exclusive Registrar for GOV.IN domain names. The use of GOV.IN Domain is restricted to the constituents of Indian Government at various levels right from Central, State/UT, District & Sub-District, block, village etc.

For detailed information and step-by-step procedure on how to register a .GOV IN Domain, one may visit http://registry.gov.in **.**

C. Link with National Portal

1) **india.gov.in:** The National Portal of India is a single window source for access to all information and services being provided by the various constituents of the Indian Government to its citizens and other stakeholders.

There are exclusive sections on Citizens, Business, Overseas, Government, Know India, Sectors etc. catering to the information needs. Sections targeting special interest groups such as Government Employees, Students, Senior Citizens, Kids etc. are also present.

a) **Since the National Portal is the official single entry Portal of the Indian Government, all Indian Government websites MUST provide a prominent link to the National Portal from the Homepage and other important pages of citizens’ interest**.

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

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

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

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

D. Content Copyright

Copyright is a form of protection provided under law to the owners of "original works of authorship" in any form or media. It is implied that the original information put up on the website by a Government Department is by default a copyright of the owner Department and may be copied, reproduced, republished, uploaded, posted, transmitted, or distributed only if the copyright policy of the concerned Department allows so.

Hence, the information, material and documents made available on an Indian Government website MUST be backed up with proper copyright policy explaining the terms and conditions of their usage and reference by others. The copyright policy of a Department could be liberal, moderate or conservative depending upon their preferences based on the kind of information available on their website. However, since it is a duty of a Government Department to provide all the information in the public domain freely to the citizens, the Departments should aim to have a liberal copyright policy.

The Departments should also be sensitive towards publishing any information having a third party copyright. The Government Departments MUST follow proper procedures to obtain the permission, prior to publishing such information on their websites.

If any published Government Document/Report is being reproduced on any website, whether as excerpts or in full, the source of the same i.e. Full Title of the Report/Document along with the name of the concerned Department and year of publication MUST be provided.

E. Content Hyper linking

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

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

a) To create a visual distinction for links that lead off site, Cascading Style Sheets (CSS) controls or XSL or some such similar mechanism should be used. In case the link takes the user to another website of the same Department/Ministry/ State, a seamless transition should be used through appropriate CSS controls.

b) Third party content should only be linked when consideration about the copyright, terms of use, permissions, content authenticity Kakinada and other legal and ethical aspects of the concerned content have been taken into account.

c) The overall quality of a website's content is also dependent, among other things on the authenticity Kakinada and relevance of the 'linked' information it provides.

d) Further, it MUST be ensured that 'broken links' or those leading to 'Page Not Found' errors are checked on a regular basis and are rectified or removed from the site immediately upon discovery.

F. Privacy Policy

Government websites should follow an extremely cautious approach when it comes to collecting personal details/information about the visitors to the sites. It should be an endeavour to solicit only that information which is absolutely necessary.

In case a Department solicits or collects personal information from visitors through their websites, it MUST incorporate a prominently displayed Privacy Statement clearly stating the purpose for which information is being collected, whether the information shall be disclosed to anyone for any purpose and to whom.

Further, the privacy statement should also clarify whether any cookies shall be transferred onto the visitor's system during the process and what shall be the purpose of the same.

Whenever a Department's website allows e-commerce and collects high risk personal information from its visitors such as credit card or bank details, it MUST be done through sufficiently secure means to avoid any inconvenience. SSL (Secure Socket Layer), Digital Certificates are some of the instruments, which could be used to achieve this.

Annex-G (Open APIs)

Policy on Open Application Programming Interfaces (APIs)

Under the overarching vision of Digital India, Government of India (GoI) aims to make all Government services digitally accessible to citizens through multiple channels, such as web, mobile and common service delivery outlets.

To meet this objective, there is a need for an interoperable ecosystem of data, applications and processes which will make the right information available to the right user at the right time.

Interoperability among various e-Governance systems is an important prerequisite for upgrading the quality and effectiveness of service delivery. For promoting Open Standards for software interoperability across various Government departments and agencies, GoI has already notified the “Policy on Open Standards for e-Governance” and “Technical Standards on Interoperability Framework for e-Governance”.

Open API is the API that has been exposed to enable other systems to interact with that system. Open API may be either integrated with the host application or may be an additional piece of software that exposes any proprietary API with an Open API equivalent. The Open API, whenever possible, may be free of charge and without restrictions for reuse & modifications.

Policy on Open APIs for Government of India” (hereinafter referred to as the “Policy”) will encourage the formal use of Open APIs in Government organizations. This policy sets out the Government’s approach on the use of “Open APIs” to promote software interoperability for all e-Governance applications & systems and provide access to data & services for promoting participation of all stakeholders including citizens.

The objectives of this policy are to:

i. Ensure that APIs are published by all Government organizations for all e-Governance applications and systems.
ii. Enable quick and transparent integration with other e-Governance applications and systems.
iii. Enable safe and reliable sharing of information and data across various e-Governance applications and systems.
iv. Promote and expedite innovation through the availability of data from e-Governance applications and systems to the public.
v. Provide guidance to Government organizations in developing, publishing and implementation using these Open APIs.

Government of India shall adopt Open APIs to enable quick and transparent integration with other e-Governance applications and systems implemented by various Government organizations, thereby providing access to data & services and promoting citizen participation for the benefit of the community.

The Open APIs shall have the following characteristics for publishing and consumption:

i. The relevant information being provided by all Government organizations through their respective e-Governance applications shall be open and machine readable.

ii. All the relevant information and data of a Government organization shall be made available by Open APIs, as per the classification given in the National Data Sharing and Accessibility Policy (NDSAP-2012), so that the public can access information and data.

iii. All Open APIs built and data provided, shall adhere to National Cyber Security Policy.

iv. The Government organizations shall make sure that the Open APIs are stable and scalable.

v. All the relevant information, data and functionalities within an e-Governance application or system of a Government organization shall be made available to other e-Governance applications and systems through Open APIs which should be platform and language independent.

vi. A Government organization consuming the data and information from other e-Governance applications and systems using Open APIs shall undertake information handling, authentication and authorization through a process as defined by the API publishing Organization.

vii. Each published API of a Government organization shall be provided free of charge whenever possible to other Government organizations and public.

viii. Each published API shall be properly documented with sample code and sufficient information for developers to make use of the API.

ix. The life-cycle of the Open API shall be made available by the API publishing Government organization. The API shall be backward compatible with at least two earlier versions.

x. All Open API systems built and data provided shall adhere to GoI security policies and guidelines.

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

The policy shall be applicable to all Government organizations under the Central Government and those State Governments that choose to adopt this policy for the following categories of e-Governance systems:

- All new e-Governance applications and systems being considered for implementation.
- New versions of the legacy and existing systems.

Annex-H (Internet of Things)

1. Sensor & Actuators

a. IEEE 1451

IEEE 1451 is a set of smart transducer interface standards developed by the Institute of Electrical and Electronics Engineers (IEEE) Instrumentation and Measurement Society's Sensor Technology Technical Committee describing a set of open, common, network-independent communication interfaces for connecting transducers (sensors or actuators) to microprocessors, instrumentation systems, and control/field networks.

b. Identification Technology

ISO/IEC JTC 1/SC31 Automatic identification and data capture techniques

It develops and facilitates standards within the field of automatic identification technologies. These technologies include 1D and 2D barcodes, active and passive RFID for item identification and OCR.

c. Domain Specific Compliance:

Sensors/IoT Devices/Actuators should follow the compliance to respective domain specific standards, like healthcare devices HL7, automobile/bus UBS-II (ITS sensor parameter & standards), OBD-II, Electric Vehicle Charging etc.

2. Communication Technology

a. Thread:

Networking protocol called Thread that aims to create a standard for communication between connected household devices.

b. AllJoyn:

Open source AllJoyn protocol was initially developed by Qualcomm provides tools for the entire process of connecting and maintaining devices on a Wi-Fi network.

c. IEEE 802.15.4:

It offers physical and media access control layers for low-cost, low-speed, low-power Wireless Personal Area Networks (WPANs).

IEEE 802.15.4e-2012, IEEE 802.15.4-2011, IEEE 802.15.4-2003, IEEE 802.15.4-2006

d. IETF IPv6 over Low power WPAN (6LoWPAN):

It defines encapsulation and header compression mechanisms that allow IPv6 packets to be sent to and received over IEEE 802.15.4 based networks.

6LoWPAN Frame Format

Fragmentation and Reassembly

Header Compression

Support for security mechanisms

e. IETF "Routing Over Low power and Lossy (ROLL):

IPv6 Routing Protocol for Low power and Lossy Networks (LLNs) (RPL)

RPL Topology Formation (Destination Oriented Directed Acyclic Graphs - DODAGs)

RPL Control Messages

f. **IETF Constrained Application Protocol (CoAP):**
It offers simplicity Kakinada and low overhead to enable the interaction and management of embedded devices.

3. **Use Case/ Application Specific:**

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

(Source: http://www.omg.org/hot-topics/iot-standards.htm)

ii. **eHealth:** IEEE has many standards in the eHealth technology area, from body area networks to 3D modeling of medical data and personal health device communications. IEEE 11073 standards are designed to help healthcare product vendors and integrators create devices and systems for disease management.

iii. **eLearning:** The IEEE Learning Technology Standards Committee (LTSC) is chartered by the IEEE Computer Society Standards Activity Board to develop globally recognized technical standards, recommended practices, and guides for learning technology.

iv. **Intelligent Transportation Systems (ITS):** IEEE has standards activities on many aspects of ITS, such as vehicle communications and networking (IEEE 802 series), vehicle to grid interconnectivity (IEEE P2030.1), addressing applications for electric sourced vehicles and related support infrastructure, and communication for charging (IEEE 1901).

4. **Consortia**

a. **Open Interconnect Consortium:**
OIC (Atmel, Dell, Broadcom, Samsung, and Wind River as members) is an open environment to support the billions of connected devices coming online.

b. **Industrial Internet Consortium:**
It was founded by Intel, Cisco, AT&T, GE & IBM with the goal of developing standards specifically for industrial use of the Internet of Things.

5. Architecture Technology

a. IEEE P2413: Standard for an Architectural Framework for the Internet of Things

The architectural framework for IoT provides a reference model that defines relationships among various IoT verticals (e.g., transportation, healthcare, etc.) and common architecture elements.

The standard also provides a reference architecture that builds upon the reference model. The reference architecture covers the definition of basic architectural building blocks and their ability to be integrated into multi-tiered systems.

6. Further Readings for Standards

a. ITU Standardization Roadmap

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

b. IERC Position Paper on IoT Standardization:

It presents an inventory of existing standards and provides an overview of past and current activity in relation to standardization in the area of Internet of Things, and assembles a series of examples of standardization activities in this area.

Annex-I (Smart Parking)

The following standards and certifications need to be followed:

1. **Entry Device**
   i. Communication protocol should be TCP/IP
   ii. Conform ISO 9001 Quality Assurance Standard
   iii. CE, FCC, IC, CNRTLUS certified
   iv. Degree of protection based on IEC 60529: IP43

2. **Exit Device**
   i. Conform ISO 9001 Quality Assurance Standard

3. **Entry/Exit Barrier**
   i. The Barrier unit must conform to ISO 9001 Quality Assurance standards
   ii. CE, Ukr - Sepro certified
   iii. Degree of protection: IP34D

4. **Sensors**
   i. Conform ISO 9001 Quality Assurance Standard
   ii. Protection Level: IP67

5. **Parking light aisle indicators**
   i. Conform ISO 9001 Quality Assurance Standard
   ii. Protection Level: IP55

6. **Indoor LED indicators**
   i. Conform ISO 9001 Quality Assurance Standard
   ii. Protection Level: IP33
   iii. Communications: Bus RS-485

7. **Other Technical Specifications**

Annex-J (Public WI-FI)

1. All equipment must support the following standards/capabilities:

i. 802.11n

ii. 802.11ac

iii. 802.11e Quality of Service (QoS)

iv. WMM Wireless Multimedia Extensions

v. WMM Power save

vi. 802.11h Dynamic Frequency Selection and Transmit Power Control

vii. 802.11i Security, including AES

viii. 802.1X with dynamic VLAN policies

ix. WPA2-Enterprise certification

x. 802.11r Roaming

xi. preferred: 3X3 MIMO

xii. preferred: Polycom/SpectraLink VIEW Certification, SpectraLink Voice Priority

xiii. preferred: Wi-Fi Certified Voice-Enterprise

2. Wireless Access points specs

i. Shall be IEEE 802.11ac compliant concurrent dual radio access point.

ii. Shall feature a three spatial-stream 802.11ac (3x3 MIMO) integrated or external dual band (2.4GHz & 5GHz) antenna.

iii. Shall have 802.3af or 802.3at compliant Gigabit PoE UTP port and a console port.

iv. Shall be IEEE 802.3af PoE compliant and both the radios shall operate at full power and full performance on 802.3af PoE/Gigabit Ethernet.

v. Shall be Wi-Fi Alliance certified for interoperability with all IEEE 802.11a/b/g/n/ac client devices.

vi. Shall support up to 16 SSID/VSC profiles.

vii. Shall support simultaneous detection & prevention of wireless threats on 2.4GHz & 5GHz frequency bands.

viii. Shall support both centrally managed mode (configured and updated via a controller) and autonomous mode (standalone in the absence of a controller).

ix. Shall support auto-selection of RF channel and transmit power.

x. Shall support enforcement of client authorization based on user credentials (802.1X/EAP), and hardware identifiers (MAC address, WEP key).

xi. Shall support ACS or similar feature to reduce co-channel interference (CCI) by automatically selecting an unoccupied radio channel.

xii. Must support Proactive Key Caching and/or other methods for Fast Secure Roaming.

xiii. AP model proposed must be able to be both a client-serving AP and a monitor-only AP for Intrusion Prevention services

xiv. Must support up to 23dbm of transmit power in both 2.4 GHz and 5 GHz radios.

xv. The Wireless AP should have the technology to improve downlink performance to all mobile devices including one-, two-, and three spatial stream devices on 802.11n. The technology should use advanced signal processing techniques and multiple transmit paths to optimize the signal received by 802.11 clients in the downlink direction without requiring feedback and should work with all existing 802.11 clients.

Annex-K (Disaster Management)

The aim of the local disaster management standards and guidelines is to support local government / municipal corporations to develop a community specific disaster management system, including governance arrangements, a Local Disaster Management Plan (LDMP) using the comprehensive approach to disaster management.

This standard establishes a common set of criteria for all hazards disaster/emergency management with fundamental criteria to develop, implement, assess, and maintain the program for prevention, mitigation, preparedness, response, continuity and recovery.

International Standards used in Disaster Warning and Management

S. No.	Standards	Description
1.	ISO 22320:2011	Societal security – Emergency management – Requirements for incident response deals with overall approach for preventing and managing emergencies /disasters
2.	ISO 22322:2015	Societal security -- Emergency management -- Guidelines for Public warning deals with guidelines for developing, managing, and implementing Public warning before, during, and after incidents / disasters
3.	ISO 22324:2015	Societal security — Emergency management — Guidelines for colour-coded alerts deals with guidelines for the use of colour codes to inform people at risk as well as first response personnel about danger and to express the severity of a situation. It is applicable to all types of hazard in any location.
4.	ISO 31000:2009, *Risk management – Principles and guidelines*	It deals with principles, framework and a process for managing risk. It helps organizations / local bodies to increase the likelihood of achieving objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment.
5.	IEC 31010:2009, Risk management -- Risk assessment techniques	It helps the decision makers understand the risks that could affect the achievement of objectives as well as the adequacy of the controls already in place. It focuses on risk assessment concepts, processes and the selection of risk assessment techniques.
6.	ISO 11320:2011	Nuclear criticality safety -- Emergency preparedness and response
7.	ASCE/SEI 41-06 *-Seismic Rehabilitation of Existing Buildings*	Standards for Seismic retrofitting of existing building including steps to better protect non-structural components (suspended ceilings, non-load-bearing walls and utility systems) and building contents (furnishings, supplies, inventory and equipment)
8.	ISO 19115-1:2014	Defines the schema required for describing geographic information and services by means of metadata. It provides information about the identification, the extent, the quality, the spatial and temporal aspects, the content, the spatial reference, the portrayal, distribution, and other properties of digital geographic data and services