Request For Proposal

for

Selection of Master System Integrator for

Varanasi Integrated Smart Solutions

RFP No.: 01/VSCL/MSI-ICT/Sep-17

Volume II: Scope of Work

Varansi Smart City Limited (VSCL), Office of Nagar Nigam, Sigra, Varanasi, UP, 221010

Contents

Preamble – Varanasi

Varanasi is the Cultural Capital of World which is popularly termed as City of Music by UNESCO. Varanasi is also known as Benares, Banaras, Kashi.

The city is known worldwide for ghats, embankments along the river bank where pilgrims perform ritual ablutions- Dashashwamedh Ghat, the Panchganga Ghat, the Manikarnika Ghat and the Harishchandra Ghat, etc. Varanasi is considered the Spiritual Centre for Hinduism and Buddhism and Jainism.

A few outlined demographics of Varanasi are:

1. Among the estimated 23,000 temples in Varanasi are Kashi Vishwanath Temple of Shiva, the Sankat Mochan Hanuman Temple, and the Durga Temple;
2. Banaras Hindu University (BHU) is One of Asia's largest residential universities;
3. Education Hub: Mahatama Gandhi Kashi Vidyapeeth, Sampooranand Sanskrit University and Tibetian University alongwith BHU
4. Climate: Varanasi experiences a humid subtropical climate;
5. Population: Varanasi urban agglomeration had a population of 16 lakhs;
6. Area: 82.10 $km^{2;}$ Elevation: 80.71 m (264.80 ft); Literacy: 80.12%.

Varanasi is governed by a number of bodies, the most important being the Varanasi Nagar Nigam (Municipal Corporation) which is responsible for the master planning of the city.

Varanasi Smart City Limited (VSCL)

The Varanasi Smart City Limited (VSCL) in the Special Purpose Vehicle (SPV) constituted as per the directives of MoUD, Govt. of India for executing SMART CITY MISSION (SCM) in Varanasi.

VSCL is led by the Divisional Commissioner, Varanasi Division of UP and works closely with the Municipal Corporation of Varanasi with the objective to achieve success in the implementation of Smart City Mission for Varanasi.

VSCL has been established under the Companies Act, 2013 of the Ministry of Corporate Affairs, Government of India. It is supported by PMC, PMU and the implementing agency for the implementation of the mission.

Vision Statement for Varanasi Smart City and Associated Objectives

The Smart City planning was done with firm belief for the cultural and spiritual importance of the city along with retrofitting of the PAN city area to rejuvenate and re-live in a smarter way through various smart solutions for Varanasi.

The vision statement is- *"To rejuvenate the oldest Indian living city of Varanasi as a great place to live and visit by conserving and showcasing its enriched heritage, culture, spirituality and traditions through innovative social and financial inclusion solutions."*

The vision is translated into various envisaged objectives for the city with various interventions to execute city operations in an integrated and a smarter way. A few broad objectives are:

- To provide Holistic Development, Administration and Operations
- Reduce congestion, air pollution
- Ensure security
- Variety of transport options - Transit Oriented Development
- Developing open spaces - parks, playgrounds, and recreational spaces
- Create Responsive Coordinative and Intelligent Ecosystem within Departments
- Improved monitoring of Utilities Operations
- Prompt Service Delivery
- (TOD) Transparent, Citizen-friendly cost effective governance
- Improved Administrative Efficiency
- Identity to the city - based on its main economic activity
- Equitable access to Public Properties
- Safe and Walkable Neighborhoods
- Pilgrim and Tourists Facilitation.

1. **Scope of Work- for Varanasi Integrated Smart Solutions (VISS)**

Overview

The Varanasi Smart City Limited (VSCL) intends to select a Master System Integrator (MSI) who will be responsible for the 'Design, Development, Implementation and Maintenance of the Varanasi Smart City – ICT Solutions' for a period of at least five (5) years, post the Go-Live date of the Overall Solution, on a turnkey basis. Under the Smart City initiative, it is envisaged to establish a Kashi Integrated Command & Control Centre (KICCC), Data center, Disaster Recovery and connect Smart elements in real time at the Varanasi City, which shall be the single & dedicated place for integrating, implementing, monitoring, controlling & commanding all City Wide Smart ICT for line departments. The Overall Scope of Work for the MSI is to provide an end-to-end ICT Solutions, which shall cater to the following primary components:

1. Kashi Integrated Command Control Center **(KICCC)**
2. Data Centre & Disaster Recovery **(DC & DR)**
3. City Surveillance System & Intelligent Traffic Management System **(ITMS)**
4. Kashi Solid Waste Management **(KSWMS)**
5. Kashi Environmental Monitoring System **(KEMS)**
6. Kashi Smart Parking Management System **(KSPMS)**
7. Kashi Smart Street Lighting Management System **(KSLMS)**
8. **GIS Maps** real time integration with Smart City Applications
9. **e-Governance**
   - Smart Kashi Portal & Smart Kashi Mobile App
   - Shri Kashi Vishwanath Temple Web site, Queue Management and Live Darshan
10. **Utilities Dashboard**
    - Water quality monitoring
    - Energy monitoring
    - Gas monitoring
11. **Helpdesk**
    - Operations Helpdesk
    - Women & Elderly Helpdesk
12. **Network from Service Providers**

The other applications that support the Management and Operations in infrastructure are Unified Communications, Integrated dashboard, Video Wall & Controller System, Operator work station, Standard

Operating Procedure Tools (SOP), Security Management, Intrusion Detection, Antivirus Management, Remote Device Management, Internet Connectivity, IT Service Management (ITSM).

It should be noted that the subsequent sections of this document detail out the expectations from the overall ICT Solution with respect to the above components. The activities defined /described/ discussed/ mentioned within this document are indicative in nature and may/may not be exhaustive. The MSI is expected to have performed an independent & in-depth analysis of any additional work(s) that may be required to be carried out to fulfil the requirements for the Overall Varanasi Smart City ICT Solutions and duly factor those in while preparing a response to this RFP. The MSI is advised to carry out detailed surveys prior to submission of the RFP response to ensure that the Bidders response caters to the complete solution, for all component requirement in order to finalize infrastructure, network bandwidth, operational & administrative challenges, etc.

2. Project Activities

Overview of Deliverables:

While this RFP lists out primary ICT objectives for catering to immediate pressing needs, keeping in view the long term scalability and sustainability of the ICT Solutions, the Bidders are encouraged to propose the State-of-Art, cutting edge ICT solutions to revive & revamp the Historic & Heritage City of Kashi using Hi-Tech solutions.

The MSI shall be responsible for carrying out the following activities:

1. Project Management
2. Survey and Detailed Design of all smart solutions components
3. Hardware Supply and Installation Stage
4. Prototype Acceptance and Factory Acceptance Testing
5. Software Development
6. System Integration
7. Testing
8. Pilot Deployment
9. Training
10. Change Management
11. Capacity Building for E-Governance

12. Final Deployment & Documentation
13. Operational System Acceptance Tests
14. Comprehensive Operations and Maintenance
15. Facility Management Staff

A. Project Management

MSI shall be responsible for end to end project management for the Implementation and Operations & Maintenance of the Kashi Smart City ICT components. MSI shall deploy a competent team of experts for Project Management which shall include a Project Manager along with a deputy project Manager. The Project Manager shall be the single point of contact that shall assume overall responsibility of the Project and ensure end to end working of the project. He shall function as the primary channel of communication for all client requirements to the implementation team. In case of any absence of the Project Manager, the MSI shall ensure that an alternate Project Manager (as approved by the client or its representative) shall be provided during the absence period. MSI shall be responsible for preparing a master schedule of work which shall highlight implementation plan for all the Project Milestones. The schedule shall identify the manufacture, delivery, installation, integration of equipment (Software and Hardware), training programs, test procedures, delivery of documentation and the respective solutions. The schedule shall include Client and any third party responsibilities along with the activities in the timeline. MSI shall conduct bi-weekly meetings between the Client, PMC and the 'key personnel' to discuss project progress & implementation in Varanasi. All key personnel associated with the project shall also be available for meetings whenever asked by the Client or its representative. MSI shall also be responsible for effective risk and issue management and escalation procedures along with matrix as part of project management. MSI shall identify, analyze, and evaluate the project risks and shall develop cost effective strategies and action plan for mitigation of risks. As part of the Project MSI shall monitor, report and update risk management plans and shall be discussed during project meetings. MSI shall prepare minutes of every meeting which takes place in the absence of PMC and submit to Client or its representative for tracking of the Project. MSI shall propose a suitable progress reporting mechanism for the project duration.

MSI will deploy Project Management Tool which should cater to effective project management, configuration management, issue and risk management, escalation procedure and matrix document repository etc. shall be factored in the proposal submitted by MSI. Based on progress reports, MSI shall also accordingly update the master schedule of work on a continuous basis during the period of the contract. Project Management plan shall be submitted to VSCL before commencing the work. The Client's representative will have at least 15 days to review and comment on every deliverable. The practice of submissions for all deliverables will be at

least one hard copies and share all the documents with PMC and VSCL stake holders. All deliveries should be approved be approved by PMC (Project Management Consultant) before submitting to Client.

B. Survey and Detailed Design of all Smart Solutions Components

MSI shall survey the site to validate the conditions provided as part of the Bid document. MSI shall conduct end-to-end survey of the site area and based on the observations asses and validate the present conditions, implementation approach and methodology, project challenges and mitigations and other project critical information. During the survey stage itself, MSI shall mobilize its entire staff and fully acquaint them with the site conditions. It is MSI's responsibilities to periodically survey the site and be updated on the conditions during the course of the contract.

During the design stage, MSI is also expected to:

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

The MSI shall be responsible for the detailed design of the Varanasi smart city solutions. MSI shall discuss in detail with the Client or its representatives the detailed design of the Varanasi Smart City Solutions and fine tune any requirements. It is the MSI's responsibility to satisfy the operational requirements of the Client and adopt industry best practices for implementation during the design stage itself. Based on the survey observation, analysis and discussion with the Client, the MSI shall submit a Detailed Design Report. The IT deliverables would include following details and not limited to System Architecture, Network Architecture, Application Architecture, Security Architecture, Routing & Switching, Integration, Operational procedures etc.

The detailed design report shall include end-to-end design validation for the project including any project understanding, analysis, detailed design, integration plan, and construction drawings. Complete set of design and construction drawing including method of installation as applicable shall also be included in the Detailed Project Report. Construction details shall accurately reflect actual job conditions.

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

Design and Construction drawings shall include the following at a minimum for drawings for all the elements as part of holistic solution:

- Overall design
- Cable requirements, routing and location (as applicable)
- Typical mounting details
- Single Line Diagrams (SLDs)
- Splicing diagrams
- Wiring diagrams
- 3D layouts and renderings
- Any other layouts
- Any other requirement to meet the requirements of the RFP for troubleshooting and maintenance

All drawings shall be updated/revised to "as-built" conditions when installation is complete.
Design submissions shall be based on project requirements and shall include as applicable, but not limited to, the following:

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

No work requiring shop drawing submission shall commence until final review has been obtained by Client. However, review of the shop drawings by the Client shall not relive the MSI of his responsibility for detailed design inherent to shop drawings. For the software components like E-Governance applications, MSI will create requirement analysis documents for various components of the solution. This includes System Requirements Specification (SRS) and Functional Requirements Specification (FRS) documentation. The MSI shall be responsible for documenting any existing/planned 'processes' of the Client as part of these deliverables.

C. Prototype Acceptance and Factory Acceptance Testing

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

Material provided as part of the Project shall undergo Prototype Acceptance Test (PAT) and Factory Acceptance Test (FAT) as per Project Plan. Details regarding the PAT and FAT are presented in Testing Section of the Scope of Work. MSI shall also present to the Client and its representatives the test results for PAT and FAT in the form of Test Result Documentation presented in the Testing section. The client at its own discretion shall visit any FAT site. MSI shall be responsible for organizing all logistics required for this site visit. For all the software components, MSI shall also propose prototype of solution components in this phase and get the required approvals.

D. Hardware Supply and Installation Stage

MSI shall be responsible for the supply and installation of all components as part of the Varanasi Smart City solutions to meet the Technical, Functional, Business and Performance requirements of this RFP. No deviations from these requirements shall be acceptable by the client. Any additional hardware or software component required to meet the technical and performance requirement of the project and not specified as part of this document but required to meet the overall requirements of the project shall be factored in as part of the Bid, and provided by the MSI. MSI shall deliver the project, install and handle the equipment in accordance with manufacturer's requirements. Installation process of the MSI shall be flexible and shall accommodate Client's requirements without affecting the schedule as specified in the RFP.

MSI shall be responsible for all supply, storage and handling of the material provided as part of the bid document. The OEM proposed for the IT infrastructure shall be in line with the national security policy (as applicable).

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

scope of MSI. The Client shall only provide raw power for all the equipment. In case of, there is NO power or insufficient power as per the requirement of the equipment, It may be considered that the new power supply connection has to be applied by MSI on the name of the client and Client will provide all necessary help to the client in procuring the Raw power.

E. Software Development

MSI shall be responsible for development and deployment of all software to meet the requirements of the project. It is preferred that MSI will use a world class Commercially Of The Shelf (COTS) or widely used software packages. However, some of the modules may require bespoke development. MSI shall be fully responsible for developing and implementing all software required for the project. This software shall be developed based on the approved software and functional requirements specifications. The technology platform chosen for all software shall be based on industry standards based and shall be secure. Migration of data shall be the responsibility of the MSI. MSI is required to take the source data in the format which is available. Subsequently, MSI is required to take complete ownership of data migration and also develop a detailed plan for data migration. MSI will create SRS for application development and get approval from VSCL for UX design before commencing development and also periodic review meetings should be scheduled for review of application and progress of the project.

All licenses for the software shall be perpetual and the client may purchase any additional licenses at the stated per unit cost (as per financial proposal of the Bidder) during this course of the contract. The MSI shall ensure that full support from the OEM's is provided during the course of the contract. All OEMS should give the Manufacturer's Authorization Form (MAFs) and other supporting documents. MSI shall be responsible to provide any upgrades, patches, fixes to the software during the course of the contract at no additional cost to the client.

System Study, Design, Development, Integration, Testing and Certification

MSI would be responsible for development, adding functionality/Customising over and above the applications (COTS product) or any bespoke software (If required) based on the unique requirements of the client (VSCL/VMC/Other Stakeholders). For the additional functionality that the client want to be added, the MSI shall carry out a detailed systems study to refine the Functional Requirements Specifications provided in this RFP and formulate the System Requirements Specifications (SRS). The study should also include different integration points of KICCC with external agencies as per client's requirement. The MSI should also prepare a detailed document on the implementation of the customised or developed product with respect to configuration,

customization and extension as per the requirement of client. The MSI would also prepare a change/reference document based on changes or deviations from the base version of the application (COTS product). The MSI will also be responsible for:

- Conducting Site preparation study for hardware, networking and office infrastructure
- Preparation of System Requirements Specifications (SRS) for additional functionalities and different integration points with External Agencies.
- Preparation of implementation document with respect to Configuration, Customization and extensions as per the requirement of client.
- Preparation of the Solution Design.
- Solution Development and/or Customization and/or Configuration and/or Extension as required.
- Development of reports.
- Formulation of test plans and test cases for additional functionalities and different integrations with external agencies.
- Preparation of Change/Reference document which will include all the changes or deviations from the base version of the product.
- Testing of the configured solution and additional functionalities.

Enhancements of functions / additions of new modules / integration requirements to various interfaces (as and when they happen) shall also be incorporated in the SRS and shall form the scope of work for the MSI.

Creation of Test Plans: - Once the SRS is approved and design is started, the MSI would prepare all necessary Test Plans (including test cases), i.e., plans for Unit Testing, Integration and System Testing and User Acceptance Testing. Test cases for UAT would be developed in collaboration with domain experts identified by the client. The Test Plans also include planning for the testing any integration with 3rd party COTS solutions, any external agencies. The Test Plans should also specify any assistance required from the client and should be followed upon by the MSI. The MSI should have the Test Plans reviewed and approved by the PMU. The client will sign off on the test plans on the advice of PMU.

High Level Design (HLD): - Once the SRS is approved, the MSI would complete the HLD and all HLD documents of the additional functionalities, integration with external agencies upon the approved SRS. The MSI would prepare the HLD and have it reviewed

and approved by the PMU. The client will sign off on the HLD documents on the advice of PMU.

Detailed (Low Level) Design (LLD): - The LLD would interpret the approved HLD to help application development and would include detailed service descriptions and specifications, application logic (including pseudo code) and UI design (screen design and navigation). The preparation of test cases will also be completed during this stage. The MSI would have the design documents reviewed and approved by the PMU. The client will sign off on the LLD documents upon the advice of PMU.

Application Development and Unit Testing: - The MSI would develop the application in accordance with the approved requirements specifications and design specifications and according to the approved Project Plan; and carry out the Unit Testing of the application in accordance with the approved test plans. The MSI would also implement the changes proposed in the Change/Reference document and carry out a thorough regression testing for the functionality. The user acceptance testing and fine-tuning of the application would be at client location. Also, the key senior resources would continue to be based on site at client location.

Regression, Integration, System and Functional Testing: - After successful unit testing of all components, the MSI would conduct full-fledged integration testing, system testing and functional testing in accordance with the approved Test Plans for the configured/customized product, additional functionalities and also integration with external agencies. This would include exhaustive testing including functional testing, performance testing (including load and stress), scalability testing and security testing. Functional testing will be led by the MSI's experts. A thorough regression testing should be conducted for those functionalities identified in Change/Reference document to provide a general assurance that no additional errors have cropped up in the process of addressing the customizations and/or Extensions. Making all necessary arrangements for testing including the preparation of test data, scripts if necessary and setup of test environment (across multiple platforms) shall be the responsibility of the MSI. The MSI along with PMU should take the responsibility in coordinating with client and other stakeholders for a smooth integration.

Test Reports: - The MSI shall create test reports from testing activities and submit to PMU for validation.

Test Data Preparation: - The MSI shall prepare the required test data and get it vetted by PMU. The test data shall be comprehensive and address all scenarios identified in the test cases. The MSI should also prepare the test data for all required integrations with external agencies.

User Acceptance Testing (UAT): - Test Plans for UAT would be prepared by the MSI in collaboration with the PMU and client nominated domain experts. The MSI will plan all aspects of UAT (including the preparation of test data) and obtain required assistance from client to ensure its success. PMU will assemble representatives from different user groups based on inputs from the MSI and would facilitate UAT. The MSI would make the necessary changes to the application to ensure that the customised/developed product successfully goes through UAT.

Final testing and certification: - The Project shall be governed by the mechanism of final acceptance testing and certification to be put into place by the Client, guided by the following principles:

- Client reserves the right to nominate a technically competent agency ("Final Testing and Certification Agency") for conducting final acceptance testing and Certification.
- Such Final Testing and Certification Agency will lay down a set of guidelines following internationally accepted norms and standards for testing and certification for all aspects of project development and implementation covering software, hardware and networking including the processes relating to the design of solution architecture, design of systems and sub- systems, coding, testing, business process description, documentation, version control, change management, security, service oriented architecture, performance in relation to compliance with SLA metrics, interoperability, scalability, availability and compliance with all the technical and functional requirements of the RFP and this Agreement.
- The Final Testing and Certification Agency will be involved with Project from the development stage to ensure that the guidelines are being followed and to avoid large scale modifications pursuant to testing done after the application is fully developed.
- The Final Testing and Certification Agency may engage professional organizations for conducting specific tests on the software, hardware, networking, security and all other aspects.

- The Final Testing and Certification Agency will establish appropriate processes for notifying the System Integrator of any deviations from the norms, standards or guidelines at the earliest instance after taking cognizance of the same to enable the System Integrator to take corrective action.
- Such an involvement of and guidance by the Final Testing and Certification Agency shall not, however, absolve the System Integrator of the fundamental responsibility of designing, customizing/ developing, installing, testing and commissioning the various components of the Project to deliver the services in perfect conformity with this Agreement.

F. System Integration

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

In case the integration of any of the systems is not as per the requirements specified in the bid document, MSI shall be responsible to provide any upgrades required to meet the integration requirements at no additional cost to the client unless otherwise agreed by the client. It shall be the responsibility of MSI to take approval of the client for the Integration of the overall system as per the bid document. Post systems integration, the client shall review and approve the overall performance of the integrated system as per the requirements of the bid document. MSI shall be responsible for fixing any requirements that are not found in compliance with the original bid requirements and approved detailed design at no additional cost to the client.

G. Testing

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

equipment, materials and systems furnished and installed function in the manner intended and in full compliance with the requirements outlined in the RFP and the approved detailed design of the MSI.

All tests shall be subject to inspection or witnessing of tests by the Client or its representative. Inspection or witnessing of tests may be waived at the sole discretion of the Client or their representative, subject to the MSI furnishing the Client or their representative with properly completed test certificates in accordance with the requirements of the RFP. Failure of the Client or their representative to witness any test shall not relieve the MSI of the obligation to meet the requirements of the Contract. MSI shall submit an Acceptance Test Procedures document (ATP), for Client's approval prior to undertaking any testing. The ATP shall clearly address:

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

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

All measuring instruments required to measure test parameters shall be calibrated by an approved testing authority. The equipment shall be inspected for standards of construction and electrical and mechanical safety. MSI will take appropriate certificate from the supplier.

Test results shall be recorded for all tests conducted under this Contract. The MSI shall make test results available to Client or their designate for review immediately after completion of the tests.
ATP for each test shall be collated, bound and delivered as part of the close-out documentation requirements specified herein. ATP submission shall include a hard copy of the originally marked test results and a neatly typed summary. One (1) hard copies and one (1) electronic copy shall be provided.

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

- **Prototype Acceptance Tests (PAT):** Prototype Approval Test shall be conducted only on the customized equipment for their design and compliance to functional specifications. PAT shall be completed before conducting FAT and only after approval of PAT by Client's representative, the equipment shall go in production. PAT shall be witnessed by Client's representatives;

- **Factory Acceptance Tests (FAT):** FAT shall be conducted before the equipment and software is shipped to Client for installation, and deficiencies shall be rectified before shipping to Client for installation. All devices furnished by the MSI shall be tested and subjected to a nominal 72-hours burn-in period at the factory. MSI will take certificate from OEMs in this regard. FAT shall be witnessed by Client's representatives at their discretion. Factory acceptance tests shall be conducted on randomly selected final assemblies of all equipment to be supplied. In case any of the selected samples fail, the failed sampled is rejected and additional 20% samples shall be selected randomly and tested. In case any sample from the additional 20% also fails the entire batch may be rejected;

- **Pre-Installation Testing (PIT):** All equipment supplied under this Contract shall undergo pre-installation testing in accordance with the ATP. This shall include existing equipment, any spare parts, any new equipment provided by Client or their designate and new equipment provided by the MSI.

  If the equipment is considered a standard production item, the MSI may, with the prior consent of the Client or their designate, supply a copy of the equipment manufacturer's quality control test results in place of a MSI performed test. All PIT testing shall be carried out prior to installation of the equipment. After satisfactory completion of the MSI's PIT tests, the MSI shall supply all test.

  All PIT testing shall be carried out prior to installation of the equipment. After satisfactory completion of the MSI's PIT tests, the MSI shall supply all test measurements and results to the Client or their designate, together with a Test Certificate.

- **Installation Acceptance Tests (IAT):** IAT shall be conducted after each installation of each equipment type, and deficiencies shall be rectified before the initiation of SAT. IAT may be witnessed by Client's representatives

- **Proof of Performance Testing (POP):** The MSI shall implement a structured proof of performance testing, which will progressively place all components in service. Site tests shall be performed on individual components, subsystem sites, and the complete subsystems, as necessary to confirm that each element of the system functions satisfactorily and fulfils the requirements of this specification.

  Completion, submission, and approval of all relevant PIT and IAT tests and results must be completed prior to carrying out any POP tests. All subsystem equipment and components shall be tested by the MSI regardless of whether or not it is a standard item.

  After satisfactory completion of the MSI's POP tests, the MSI shall supply all test measurements and results to the Client or their designate, together with a Test Certificate.

- **System Integration Testing (SIT):** The MSI is responsible for the proper and harmonious operation of all subsystems installed under this Contract. Where connections of the new systems to existing subsystems or equipment supplied by others are required, the MSI is responsible for connection of equipment specified in the Contract and for initial system integration tests. Such a test will verify the full functionality of each subsystem as they are interconnected. This will require testing to be coordinated by the MSI with the Client or their designate. This work will be carried out under the direction of the Client or their designate.

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

The MSI shall:

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

A SIT certificate will be issued when all system tests have been completed satisfactorily, and the MSI has supplied a full set of Test Certificates and a Test Certificate for the complete system, together with final copies of all Operating and Maintenance Documentation for the System.

Stress and Load Testing: Comprehensive stress and load testing of e-Governance and Smart elements applications shall be conducted to demonstrate robustness and reliability of the system where necessary like Surveillance, Vehicle Tracking for SWM, Mobile App users etc.

Security Testing (including penetration and vulnerability test): Security test shall be conducted to demonstrate security requirements at network layer and software applications. Components shall pass vulnerability and penetration testing for rollout of each phase. Components shall also pass web application security testing for portal, Mobile App, and other systems. Security testing shall be carried out for exact same environment/architecture that shall be set up for go-live. Penetration test shall be carried out periodically and vulnerability analysis shall be carried half-yearly during maintenance phase. For all applications hosted on-cloud or hosted on premises, the security testing shall be a mandatory requirement.

Pilot Test: Requirements for Pilot Test is explained in the Pilot Deployment Section of the Scope of Work.

System Acceptance Tests (SAT): SAT shall be conducted after the entire system has been installed, integrated and commissioned. Deficiencies, if any shall be rectified before the initiation of Burn-in Test. SAT shall be conducted on full system completion only to determine if the system functional and technical requirements as specified in the bidding documents are meet. SAT shall be witnessed by Client's representatives. Data migration, if any will be carried out by ST prior to commencement of this stage. SAT shall also include any performance and load testing for the software applications.

Burn-in Tests (BT): Following successful completion of the SIT and SAT, the approved System will be put into service and its performance monitored for a period of thirty (30) consecutive calendar days for the purpose of verifying system reliability in an operating environment. Any failures and defects occurring in this time will be documented. Any serious defects which affect the availability of the system will be a basis for restarting the test. Upon the satisfactory completion of this performance testing a Completion Certificate will be issued.

The MSI shall not commence BT until SIT and SAT have been performed and successfully completed and all documentation of the successful completion of PAT, FAT, PIT, IAT, POP, SIT and SIT, along with notification of the schedule date of the BT is provided to the Client or their designate in accordance with the

requirements. Commencement of BT will be conditional on the Client or their designate providing written notification of Client's readiness to proceed to BT.

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

Where equipment supplied by the MSI fails during the burn-in period, the MSI shall restart the test at day zero (0) following appropriate corrective measures.

If a utility failure is proved to be the cause of testing failure, then the MSI shall restart the fourteen (14) day burn-in test at the day the failure occurred. If a subsystem failure is proved to be the cause of testing failure, then the MSI shall start the test over at day 0 (zero).

Where tests or burn-in indicate that an existing subsystem or component, not provided by the MSI, is defective, the MSI shall immediately report the deficiency to the Client or their designate. The Client or their designate may assign corrective repairs, retesting and repeat of BT to the MSI, in accordance with change provisions of the Agreement.

The MSI shall provide the Client or their designate with a contact name and phone number(s) for a designated emergency contact person during BT. The emergency contact person shall be accessible twenty-four (24) hour a day, for each day of testing.

Issuance of the Completion Certificate is a basis for the start of the Warranty period for the Systems.

Operational Acceptance Test: shall be conducted after successful SAT and Burn-in tests. Continuous fault free running of the System shall be tested. Post the completion of Operational Acceptance Test, System shall be considered for Operational System Acceptance and Defect Liability Period (DLP) shall commence. Operational Acceptance Test shall include the following as a minimum:

- Completion of all activities and fulfilment of all business, functional and technical requirements listed in RFP
- Scrutiny of all inspection reports, audit findings, Contracts, licensing agreements etc.

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

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

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

<table>
<tr><td colspan="2">Item #</td><td colspan="2">Date</td></tr>
<tr><td colspan="2">Item Description</td><td colspan="2">Tester</td></tr>
<tr><td colspan="2">Test</td><td colspan="2"></td></tr>
<tr><td colspan="3">Test Setup:</td><td></td></tr>
<tr><td>Clause</td><td>Test Procedure</td><td>Expected Results</td><td>Actual Results</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="4">Witnessed: (This Does Not Constitute Approval) Reviewed and Approved:</td></tr>
</table>

MSI shall be responsible to carry out all the testing as per the satisfaction of the Client and its representatives. All the costs those are associated with any testing are to be borne by the MSI including the costs of travel and accommodation of the Client or its representatives from their home locations in their cost bid. In the interest of the MSI maximum of three (3) people shall be nominated by the Client to attend any such testing wherever it is carried out. In case of failure of any testing, the failure component shall be repaired and the test shall be rerun. If a component has been modified as a result of failure, that component shall be replaced in all like units and the test shall be rerun for each unit.

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

H. Pilot Deployment

The MSI shall conduct Pilot deployment and testing for meeting Client's business requirements before rolling out the complete system. The pilot will be run for four weeks to study any issues arising out of the implementation. MSI shall also review health, usage and performance of the system till it is stabilized during pilot deployment. Based on Client's feedback for incorporating changes as required and appropriate, MSI shall train staff involved in the Pilot implementation.

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

I. Third Party Acceptance Testing, Audit and Certification

The primary goal of Acceptance Testing, Audit & Certification is to ensure that the system meets requirements, standards, and specifications as set out in this RFP and as needed to achieve the desired outcomes. The basic approach for this will be ensuring that the following are associated with clear and quantifiable metrics for accountability:

- Functional requirements
- Test cases and Requirements Mapping
- Infrastructure Compliance Review
- Availability of Services in the defined locations
- Performance and Scalability
- Security / Digital Signatures
- Manageability and Interoperability
- SLA Reporting System
- Project Documentation
- Data Quality Review

As part of Acceptance testing, audit and certification, performed through a third party agency, VSCL shall review all aspects of project development and implementation covering software, hardware and networking including the processes relating to the design of solution architecture, design of systems and sub-systems, coding, testing, business process description, documentation, version control, change

management, security, service oriented architecture, performance in relation to defined requirements, interoperability, scalability, availability and compliance with all the technical and functional requirements of the RFP and the agreement. Here, it is important to mention that there may be two agencies selected, one for audit & certification of security and control aspect of the system and the other for audit & certification of overall application S/w. VSCL will establish appropriate processes for notifying the MSI of any deviations from defined requirements at the earliest instance after noticing the same to enable the MSI to take corrective action. Such an involvement of the Acceptance Testing & Certification agencies (STQC/CERT-IN Empanelled Agency), nominated/appointed by MSI with prior approval of VSCL, will not, however, absolve the MSI of the fundamental responsibility of designing, developing, installing, testing and commissioning the various components of the project to deliver the services in perfect conformity with the SLAs. Following discusses the acceptance criteria to be adopted for system as mentioned above:

- **Functional Requirements: -** The system developed/customized by MSI shall be reviewed and verified by the agency against the Functional Requirements signed-off between VSCL/Concerned Department Authority and MSI. Any gaps, identified as severe or critical in nature, shall be addressed by MSI immediately prior to the deployment of the system in production. One of the key inputs for this testing shall be the traceability matrix to be developed by the MSI from system. Apart from Traceability Matrix, agency may develop its own testing plans for validation of compliance of system against the defined requirements. The acceptance testing w.r.t. the functional requirements shall be performed by both independent third party agency (external audit) as well as the select internal department users (i.e. User Acceptance Testing).

- **Infrastructure Compliance Review: -** Third party agency shall perform the Infrastructure Compliance Review to verify the conformity of the Infrastructure supplied by the MSI against the requirements and specifications provided in the RFP and/or as proposed in the proposal submitted by MSI. Compliance review shall not absolve MSI from ensuring that proposed infrastructure meets the SLA requirements.

- **Security Review: -** The software developed/customized for system shall be audited by the agency from a security & controls perspective. Such audit shall also include the IT infrastructure and network deployed for system. Following are the broad activities to be performed by the Agency as part of Security Review. The security review shall subject the system for the following activities:
    a) Audit of Network, Server and Application security mechanisms

b) Assessment of authentication mechanism provided in the application /components/ modules
c) Assessment of data encryption mechanisms implemented for the solution
d) Assessment of data access privileges, retention periods and archival mechanisms
e) Server and Application security features incorporated etc.

- **Performance: -** Performance is another key requirement for system and agency shall review the performance of the deployed solution against certain key parameters defined in SLA described in this RFP and/or agreement between VSCL and MSI. Such parameters include request-response time, work-flow processing time, concurrent sessions supported by the system, Time for recovery from failure, Disaster Recovery drill etc. The performance review also includes verification of scalability provisioned in the system for catering to the requirements of application volume growth in future.
  a) The MSI must provide System and Database Performance System for all servers in the Data centre
  b) The MSI must provision for End-User response time monitoring and transaction based deep-dive analysis for Web based applications.
  c) The MSI must provision for Integrated Performance Management System for Monitoring Networks, Systems & Databases.
  d) The MSI must provide a Traffic Analysis and Reporting System for deep-dive diagnostics.

- **Availability: -** The system should be designed to remove all single point failures. Appropriate redundancy shall be built into all the critical components to provide the ability to recover from failures. The agency shall perform various tests including network, server, security, DC/DR fail-over tests to verify the availability of the services in case of component/location failures. The agency shall also verify the availability of services to all the users in the defined locations. The MSI would need to provide an Infrastructure Fault Management System for the following functions:
  a) Infrastructure Fault Analysis
    1. The proposed solution must automatically discover manageable elements connected to the network and map the connectivity between them. The Network Fault Management consoles must provide the topology map view from a single central console.
    2. The proposed system must support multiple types of discovery including IP range discovery, Seed router based discovery & Trap-Based Discovery

3. The system should provide discovery & inventory of heterogeneous physical network devices like Layer-2 & Layer-3 switches, Routers and other IP devices and do mapping of LAN & WAN connectivity with granular visibility up to individual ports level.
4. The system must be able to support mapping and modeling of the infrastructure grouped by network connectivity, physical location of equipment and user groups or departments
5. The system should support maps grouped by network topology, geographic locations of the equipments and user group/departments. These should help in understanding physical Network, virtual Network services and the relationships between them.
6. The system must provide visualization tools to display network topology and device to device connectivity. The system must also be able to document connectivity changes that were discovered since the last update.
7. The proposed solution must provide a detailed asset report, organized by vendor name and device, listing all ports for all devices. When a report is run the administrator must have an option of specifying the number of consecutive days the port must be —unused‖ in order for it to be considered —available.
8. The proposed solution should provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause analysis.
9. It should have a strong event correlation engine which can correlate the events on the basis of event pairing, event sequencing etc.
10. The system must be able to "filter-out" symptom alarms and deduce the root cause of failure in the network automatically.
11. The proposed solution must support a an architecture that can be extended to support multiple virtualization platforms and technologies

b) Configuration Management for Critical Network Devices

1. The system should be able to clearly identify configuration changes as root cause of network problems
2. The proposed fault management solution must able to perform real-time or scheduled capture of device configurations
3. The proposed fault management solution must able to store historical device configurations captured in the database and thereby enable comparison of current device configuration against a previously captured configuration as well as compare

the current configuration against any user-defined standard baseline configuration policy.

c) Advanced IP Services Management for technologies like QoS and Multicast

1. The proposed solution should be able to support response time agents to perform network performance tests to help identify network performance bottlenecks.
2. The proposed solution should be able to monitor QoS parameters configured to provide traffic classification and prioritization for reliable VoIP transport. The proposed solution should discover and model configured QoS classes, policies and behaviours.
3. The proposed solution should provide the ability to discover, map & monitor multicast sources & participating routers wherein the system should be able visualize the distribution tree in the topology map.

d) Infrastructure-based SLA Management and Integration Requirements

1. The proposed service management system should provide a detailed service dashboard view indicating the health of each of the departments / offices in the organization and the health of the services they rely on as well as the SLAs.
2. The system must be capable of managing IT resources in terms of the business services they support, specify and monitor service obligations, and associate users/Departments/ Organizations with the services they rely on and related Service/Operational Level Agreements.
3. Root cause analysis of infrastructure alarms must be applied to the managed Business Services in determining service outages. SLA violation alarms must be generated to notify whenever an agreement is violated or is in danger of being violated.
4. The system must provide the capability to designate planned maintenance periods for services and take into consideration maintenance periods defined at the IT resources level. In addition the capability to exempt any service outage from impacting an SLA must be available.
5. The proposed NMS should provide unified workflow between the fault and performance management systems including bi-directional and context-sensitive navigation

6. The system must support seamless bi-directional integration to helpdesk or trouble ticketing system
7. The proposed network fault management system should integrate with the helpdesk system by updating the Asset with CI information to support viewing history or open issues in helpdesk on the particular managed asset and associate an SLA to the ticket in the helpdesk.

- **Manageability Review: -** The agency shall verify the manageability of the system and its supporting infrastructure deployed using the Enterprise Management System (EMS) proposed by the MSI. The manageability requirements such as remote monitoring, administration, configuration, inventory management, fault identification etc. shall have to be tested out.

- **SLA Reporting System: - M**SI shall design, implement/customize the Enterprise Management System (EMS) and shall develop any additional tools required to monitor the performance indicators listed under SLA prescribed in this RFP. The Acceptance Testing & Certification agency shall verify the accuracy and completeness of the information captured by the SLA monitoring system implemented by the MSI and shall certify the same. The EMS deployed for system, based on SLAs, shall be configured to calculate the monthly transaction-based payout by VSCL to MSI. The MSI may provide an end to end Service Level Management System for the Data center and Network Infrastructure
  1. Provide end-to-end, comprehensive, modular and integrated management of IT infrastructure components to maximize the availability of IT services and SLA performance.
  2. The management system needs to aggregate events and performance information from the domain managers and tie them to service definitions. This capability is critical for the administrators to have a complete view of the performance and availability of various application services being managed.
  3. The proposed tools should automatically document problems and interruptions for various IT services offered and integrate with the service level management system for reporting on service level agreements (SLAs).
  4. The system must be capable of managing IT resources in terms of the business services they support, specify and monitor service obligations, and associate users/Departments/ Organizations with the services they rely on and related Service/Operational Level Agreements.
  5. Provide a detailed service dashboard view indicating the health of each of the departments / offices in the organization and the health of the services they rely on as well as the SLAs.

6. Provide a high level view for executives and other users of the system using a real time business services Dashboard.
7. Provide an outage summary that gives a high level health indication for each service as well as the details and root cause of any outage.
8. Support for a User Definition Facility to define person(s) or organization(s) that uses the business Services or is a party to a service level agreement contract with a service provider or both. The facility must enable the association of Users with Services and SLAs.
9. The Service Level Agreements (SLAs) definition facility must support defining a set of one or more service Guarantees that specify the Service obligations stipulated in an SLA contract for a particular time period (weekly, monthly, and so on). Guarantees supported must include one that monitors service availability (including Mean Time to Repair (MTTR), Mean Time between Failure (MTBF), and Maximum Outage Time thresholds) and the other that monitors service transaction response time.
10. SLA violation alarms must be generated to notify whenever an agreement is violated or is in danger of being violated.
11. Provide the capability to designate planned maintenance periods for services and take into consideration maintenance periods defined at the IT resources level. In addition the capability to exempt any service outage from impacting an SLA must be available.
12. A historical reporting facility that will allow for the generation of on-demand and scheduled reports of Business Service related metrics with capabilities for customization of the report presentation.

A List of SLAs that needs to be measured using the proposed monitoring tools is given below. These SLAs must be represented using appropriate customizable reports to ensure overall service delivery.

1. **Service Level Category: Network Infrastructure**

a) Network Specific SLAs

- Uptime SLA
- MTBF (Mean Time Between Failures) & MTTR (Mean Time to Repair)
- Latency & Response Time (DNS / DHCP / SMTP etc)
- Traffic-based SLAs

2. **Service Level Category: Data Center IT Infrastructure**

b) System Specific SLAs

- System Availability
- System Response Time
- Utilization based SLAs (CPU / Memory etc.)

3. **Application Specific SLAs**

c) End-User Based SLAs

- End-to-End Response Time for End-User Web Pages to Load
- Avg. Response Time, Errors Per Interval, Response per Interval
- SLAs from Critical Processes (e.g. Submit Button Click, Upload Action in Portal)

4. **Transaction Based SLAs**

- SLAs for Business Process involving with multiple steps / pages
- Completion Time SLA for Critical Business Processes

5. **Application Deep-Dive SLAs**

- Application Component-Wise SLA within the DC
- SLA for DB Query to Complete
- Web Services Call etc.
- 3rd Party interaction SLAs between Applications

- **Project Documentation: -** The Agency shall review the project documents developed by MSI including requirements, design, source code, installation, training and administration manuals, version control etc. Any issues/gaps identified by the Agency, in any of the above areas, shall be addressed to the complete satisfaction of VSCL.

- **Data Quality: -** The Agency shall perform the Data Quality Assessment for the Data digitized/ migrated (If required) by MSI to the system. The errors/gaps identified during the Data Quality Assessment shall be addressed by MSI before moving the data into production environment, which is a key mile stone for Go-live of the solution.

J. Training

Post the system integration, MSI shall train Client representatives to operate the equipment installed and to conduct any routine diagnostics and routine maintenance work. Training shall be done during Pilot Deployment and before Final Deployment. The period of training shall be mutually agreed upon by Client and MSI.

The MSI shall provide training courses for at least:

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

The actual number of each of above categories of trainees will be provided at Design Stage.

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

The Training Plan (TP) shall be developed for each component/module and shall include the training schedule and course outlines. Bidder must be provided to Client the TP for review at least three weeks in advance of the start of training. The TP must be approved by Client before the start of training.

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

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

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

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

The MSI shall provide brief refresher versions of each training course to the original trainees and new inductees between three to six months after System Acceptance for each deployment stage at no additional cost. A team of trainers shall be deployed fulltime for one month around the Go-Live period for each component for training the staff and stakeholders.

In addition to the training to the operations staff during system deployment stage, the MSI shall conduct half-yearly training refreshment sessions to train the new staff inducted by the Client and to enhance the knowledge of the Client's staff operating the Varanasi Smart City solutions by adopting "train the trainer" approach.

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

K. Change Management

MSI shall help the agencies with complete Change Management exercise needed to make this project a success. In fact, Change Management will have to subsume 'training' as a key enabler for change. Following outlines, the responsibilities of MSI with respect to designing and implementation of change management plan for the Project.

- Change Management initiative, to be designed & implemented by MSI, shall focus on addressing key aspects of Project including building awareness in personnel on benefits of new system, changes (if any) to their current roles & responsibilities, addressing the employee's concerns & apprehensions w.r.t. implementation of new system and benefits that are planned for the employees.

- It is required that if MSI doesn't operate in the Change Management, Communication and Training domain then he collaborates with/ hires services of a specialist agency who will be responsible for complete Change Management, Awareness and Communication implementation and monitoring, on the lines suggested below

- The agencies requiring change management as part of the project shall form various stakeholder groups to address the Change Management Initiative. Stakeholders are all those who need to be considered in achieving the project goals and whose participation and support are crucial to its success. A key individual stakeholder or stakeholder group is a person or group of people with significant involvement and/or interest in the success of the project.

- Stakeholder analysis identifies all primary and secondary stakeholders who have an interest in the issues with which the Kashi Integrated Command & Control Center is concerned. The stakeholder groups will be the set of core users (Change Agents) who will directly participate in the awareness and communication initiatives, workshops, and provide feedback to the governance Committee

- Stakeholder groups can be categorized into below categories, based on their influence and role in managing the change and making it successful:

L. Capacity Building for E-Governance

Capacity Building is a highly critical component of the project and specifically for E-Governance & implementation. The objective of the Capacity Building (CB) initiatives is to empower the direct users and other stakeholders of VMC to optimally use the system and enhance outcomes in customer facing and other core municipal functions; and also ensure a smooth functioning of VMC.

The System Integrator would render Capacity Building services in both areas, as per the "bundling" approach. The MSI holds the responsibility for creation of training material, designing the training programs and their delivery to the target group.

Building capacities at various levels is critical to the successful implementation of the recommended IT initiatives. Also, the training programs would cover at minimum general/basic computer awareness programs in addition to project-specific programs in order to ensure adoption of the system at the VMC.

The main challenges to be addressed effectively by the MSI are the diverse trainee base, wide variability in education and computer proficiency and minimal availability of time. The MSI holds the responsibility for creation of a detailed and effective training strategy, user groups and classifications, training plan and guidelines, detailed training material, training program designed their delivery to the target groups.

It has been envisaged to train approximate 50% of VMC personnel staff as a part of capacity building during the Integrated Command Control Center implementation phase. The MSI holds the responsibility for

creation of training material, designing the training programs and their delivery to the target group. Following is the indicative list of the training programs that needs to be administered to the group of officials as identified above. The overall responsibility of administering the training program lies with the MSI.

- Awareness and sensitization of benefits of IT
- Basic Computer Awareness & Role based training for application users
- Trainers Training
- System Administration & Support Training

The MSI shall be responsible for the following activities as part of the End User and Train the Trainer Training.

M. Develop Overall Training Plan

MSI shall be responsible for finalizing a detailed Training Plan for the program in consultation with VMC covering the training strategy, environment, training need analysis and role based training curriculum. MSI shall own the overall Training plan working closely with the VMC Training team. VSI shall coordinate overall training effort.

N. Develop Training Schedule and Curriculum

System Integrator shall develop and manage the training schedule in consultation with VMC, aligned with the overall implementation roadmap of the project and coordinate the same with all parties involved. Training schedule shall be developed by solution and shall be optimized to reduce business impact and effective utilization of Training infrastructure and capacities. The training curriculum for the VMC training program should be organized by modules and these should be used to develop the training materials. The training curriculum outlines the mode of delivery, module structure and outline, duration and target audience. These sessions should be conducted such that the users of the application/modules are trained by the time the application "goes-live" with possibly no more than a week's gap between completion of training and going live of modules. Continuous reporting (MIS) and assessment should be an integral function of training. MSI shall also identify the languages to be used by the end-user for entering data and ensuring multi- language training to the end users as per requirement.

O. Learning Management System and Training Portal

Developing a Learning Management System and Training Portal for providing access to all training content online including documents, demo, audio, video, simulation and practice, assessment, self-learning and context sensitive help and monitoring, support and reporting.

P. Develop Training Material

Based on the specific needs and the objectives of VMC, training programs should be organized by the MSI. The training program must include training on each of the KICCC modules.

Following is the indicative list of the training programs that needs to be administered to the group of officials as identified above. The overall responsibility of administering the training program lies with the MSI.

- Basic IT skills and use of computers to creating awareness about the benefits of ICT and basic computer skills
- Role-based training on the COTS based/ eGovernance applications – Basic and Advanced. This training should be in a role based, benchmarked and standardized format, multi-lingual and lead to learning completion and assessment. It should also allow for self-learning and retraining. Training would include mechanism for demonstration using audio / video / simulated / demo practice exercises and evaluation of trainees. The training should be module based
- System Administrator training: a few members of the various departmental staff with high aptitude would be trained to act as system administrators and troubleshooters for the system.
- Customization of the Training Manuals, User Manuals, Operational and Maintenance Manuals provided along with the Software

PLEASE NOTE: The number of training groups will depend on the number of user groups and has to be mutually decided between Client and MSI.

The minimum indicative level content for the training programs under capacity building and is listed as below:

SL No.	Type of Training	Training Content	Days (minimum)
1	**Awareness and sensitization of benefits of ICT**	This module shall cover Principles of e-governance; it shall also cover the advantages of use of ICT in VMC. It shall briefly cover the technology trends and how it can be put to use by use of live examples of ICT use across the world	2
2	**Basic computer awareness**	This module shall cover the fundamental concepts of Computer, Internet, Peripherals, System software and Application Software It shall also cover the use of MS- Office suite in detail. It can also touch upon use of office tools such as printers, fax machine, copiers and scanners as well as basics in use of computers (checking network connections, etc.).	5
3	**Role based system training on The KICCC Application Software**	This module is required to train the at various levels in operating the application. The training is to be provided to the staff depending upon their role and responsibilities in the workflow. During this training, the trainees could also be asked to carry out the routine functions using the software. The training should be module based and cover all modules of KICCC	5
4	**System Administration support and Trouble Shooting**	Skills in Troubleshooting vis-à-vis application, standard software and networking (for those with the aptitude and/or prior training)	3

In cases where the training material may be made available by the OEM, it is the MSI's responsibility to ensure the relevance of the material to MC, customize if necessary and own up the delivery and effectiveness. MSI shall ensure that the training content meets all the objectives of the training course. The material shall be developed in Hindi and English language. MSI shall also develop the training material for delivery through Computer Based Training, Instructor Led Training, Online User Material/Help Manuals and Job Aids. MSI shall provide detailed training material providing step-by-step approach in soft and hard copies to all offices for reference.

Q. Deliver Training to End Users

MSI shall deliver training to the end users utilizing the infrastructure at the designated Training Centers. Role-based training for the Senior Officers will be carried out for a suitable location by the System Integrator.

MSI shall also impart simulated training on the actual application with some real life like database. The MSI should create case studies and simulation modules that would be as close to the real life scenario as possible. The objective of conducting such trainings would be to give firsthand view of benefits of using the system. Such specialized training should also be able to provide the participant a clear comparison between the old ways of operation against the post -e-gov scenario. This training needs to be conducted by the MSI at the very end when all the other trainings are successfully completed.

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

An ILT course will have the following components

- Course Presentation (PowerPoint)
- Instructor Demonstrations (The KICCC - Application training environment)
- Hands-on Exercises (The KICCC - Application training environment)
- Application Simulations: Miniature version of The KICCC Application with dummy data providing exposure to the officers to a real life scenario post implementation of the KICCC
- Job Aids (if required)
- Course Evaluations (Inquisition

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

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

R. Deliver Training to Trainers (Internal & External – if specified by VMC)

MSI shall help VMC in assessing and selecting the internal trainers as well as external trainers who can conduct the end user training subsequent to the training by the MSI. MSI shall coordinate the 'Train the Trainer' session for the identified trainers to ensure that they have the capability to deliver efficient training.

In addition to the training delivered to the end-users, the trainers should also be trained on effectively facilitate and deliver training to end users. Also, it is advisable to always run pilots for any training program before deployment. This training will hence serve as the pilot and as a training session for trainers as well.

In addition, the end-user training sessions, Training of Trainers training will consist of three segments:

- The first segment will be set of workshops covering effective presentation skills and coaching techniques and discussing the benefits and structure of the trainer model.
- The second segment will be the formal The KICCC training which will consist of all modules relevant for their role.
- The third segment will be a teach-back session where trained trainers will present course content and receive feedback regarding content, flow, and presentation techniques. This will also include a feedback session where trainers can provide feedback on the training materials, flow, comprehension level, and accuracy.

S. Training Effectiveness Evaluation

MSI shall evaluate the effectiveness of all end user's trainings using electronic or manual surveys. MSI shall be responsible for analyzing the feedback and arrange for conducting refresher training, wherever needed. State will periodically monitor the training effectiveness through the performance metrics and Service levels and the MSI shall comply with the same.

T. Final Deployment and Documentation

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

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

All installation drawings shall be prepared in AutoCAD, GIS and Adobe Acrobat and provided on CD-ROM as well as hard copies. The drawings shall contain sufficient detail including but not limited to equipment dimensions, interfaces, cable details, equipment mounting and fire protection. Electrical and electronic drawings shall be supplied to show engineering changes made to any component or module any time during the contract period.

'As-built' Documents delivered by the MSI shall include:

- An inventory of all components supplied including model name, model number, serial number and installation location
- An inventory of all spare parts supplied including brand, model number, and serial number and storage location
- All reference and user manuals for system components, including those components supplied by third parties
- Point of Contact for each OEM for maintenance
- Warranties and Maintenance schedules for the hardware procured
- All warranties documentation, including that for components supplied by third parties
- As-built in CAD and GIS
- A diagram indicating the as-built inter-connections between components
- Software documentation which also includes the version number of all software, including that supplied by third parties
- Cable run lists and schedules
- All network and equipment details such as IP addresses, user names, and passwords
- Data communication protocols; and
- 'As-Built' drawings for all components installed

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

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

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

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

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

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

Documentation of processes shall be done using standard flow charting software. An intuitive online learning tool depicting standard operating procedures of system usage are required to be deployed.

There shall be a provision of training system in the deployment architecture so as new employees can be inducted easily.

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

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

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

U. Operational System Acceptance

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

V. Comprehensive Maintenance for System and Services

MSI shall be responsible for comprehensive maintenance of both hardware and software, required up-gradations in the system, expansion of the system, technical manpower, spares management and replenishment, performance monitoring and enhancements of the Varanasi Smart City solutions deployed as part of this project and shall maintain service levels as defined in the RFP. All equipment and material supplied by the MSI shall be provided with standard warranty against defects of design and manufacturing and against faults and failures associated with workmanship of MSI and its sub-contractors commencing from operation acceptance of the system. All equipment found to be defective during comprehensive maintenance shall be repaired or replaced by the MSI at no cost to the Client.

MSI shall provide all the technical, managerial, and other staffing required to manage day to-day maintenance of the Varanasi Smart City solutions during the Contract period. MSI shall deploy project manager stationed at Varanasi who shall be the single point of contact to the client and shall be responsible for operation and maintenance of the system.

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

MSI shall maintain all data regarding entitlement for any upgrade, enhancement, refreshes, replacement, bug fixing and maintenance for all project components during Warranty. MSI shall be responsible for updates/upgrades and implementation of new versions for software and operating systems when released by the respective OEM at no extra cost to the Client during entire duration of contract. Requisite adjustments / changes in the configuration for implementing different versions of system solution and/or its components shall also be done by MSI. The MSI shall also ensure application of patches to the licensed software covering the appropriate system component software, operating system, databases and other applications. Software License management and control services shall also be conducted by the MSI during this phase. Any changes/upgrades to the software during comprehensive maintenance shall be subjected to comprehensive and integrated testing by MSI to ensure that changes implemented in system meets the specified requirements and doesn't impact any other function of the system. Issue log for errors and bugs identified in the solution and any change done in solution (vis-à-vis the FRS, BRS and SRS signed off) shall be periodically submitted to the Client. MSI shall also be responsible for operating City website, city portal, and city application including all support, content updates and upgrades throughout the duration of contract.

Periodically, IT audits will be conducted by VSCL/ PMC during the support period.

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

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

- High level design of system;
- Module level design of system;
- System Requirement Specifications (SRS);
- Any other explanatory notes about system;
- Traceability matrix;
- Compilation environment

MSI shall also ensure Updation of following documentation of software system

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

The communication costs (Internet charges, telephone charges, 3G/GPRS connectivity charges) and any other incidental charges related to maintenance period shall be in the scope of the MSI and considered to be included in the proposal submitted by the MSI for the entire contract duration. Any planned and emergency changes to any component during maintenance period shall be through a change management process. For any change, MSI shall ensure

- Detailed impact analysis;
- Change plan with roll back plan;
- Appropriate communication on change required has taken place;
- Approvals on change;
- Schedules have been adjusted to minimum impact on production environment;
- All associated documentation is updated post stabilization of the change;
- Version control maintained for software.

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

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

W. Support Staff Required

Three (3) types of support staff shall be provided by MSI during Operations and Maintenance phase:

- Maintenance Support Staff
- Helpdesk Support staff
- Facility Management Staff

Maintenance Support Staff

Well trained, efficient and effective Maintenance Support Staff shall be provided by the MSI during the maintenance phase of the project to support Client's operational and technical requirements in day to day operations of the smart city solutions provided by MSI. Any fault originating for the Varanasi smart city components shall be addressed by the MSI Maintenance Support staff in the least time possible. The staff assigned shall be well qualified to attend to the emergency situations and shall be able to communicate in an effective and efficient manner. The supports staff shall provide 24*7 services, work in a shift based system and provide full support coverage of the Varanasi smart city solution and maintain the system as per the SLA's defined.

At a minimum, 14 maintenance personnel shall be deputed during Maintenance phase in the following shifts:

- One (1) shift of twelve hours comprising of 3 personnel each;
- One (1) shift comprising of 1 personnel.

The KICCC Operators shall be well trained on all the smart city components to understand and take necessary action in any kind of situation

Helpdesk Support Staff

MSI shall also depute support staff at Helpdesk. The support staff at Helpdesk shall provide 24*7 services, work in a shift based system and provide full support coverage of Helpdesk and maintain the system as per SLAs defined. At a minimum, 6 support personnel shall be deputed at Helpdesk during maintenance phase in following shifts:

- Two (2) shifts comprising of 2 personnel each;
- One (1) Night shift comprising of 1 personnel each

Facility Management Staff

Facilities management which include but not limited to building and grounds maintenance, cleaning, catering and vending, security, space management, utilities management etc. and associated manpower shall also be under the scope of the MSI during maintenance phase. At a minimum, MSI shall depute Facility Management staff of 9 personnel which shall work in a shift based system to provide 24*7 services. Staff requirement per each shift is as per below:

- Two (2) shifts comprising of 4 personnel each;
- One (1) Night shift comprising of 1 personnel each.

Any additional staff required for management, HR, payroll etc. of Maintenance staff, Helpdesk and Facility Management staff, if required by MSI, shall also be under the scope of the MSI.

3. GENERAL REQUIREMENTS

a) The MSI is required to draft / prepare and then finalize the detailed architecture for the overall ICT systems for the Smart City features, by incorporating findings of site surveys. The Solution so envisaged by the MSI should be able to **provide real time Kashi Integrated Command and Control Center (KICCC)**. All the components & Sub-Components of the Overall Smart City Solution and the respective Technical Architecture should:

- at least comply with the published e-Governance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and

- be of leading industry standards

While responding to the RFP, the Bidders are to submit the detailed Technical Architecture for all the components along with the detailed description of each of the Smart City ICT Component, their Sub-Components. The Solution should factor in and 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 the Varanasi City. The system should also support vertical and horizontal scalability so that depending on changing requirements from time to time, the system may be scaled upwards. There must not be any system imposed restrictions on the upward scalability in number of cameras, data centre equipment or other smart city components. Main technology components requiring scalability are storage, bandwidth, computing performance (IT Infrastructure). The architecture should be scalable (cater to increasing load of internal and external users and their transactions) and capable of delivering high performance till the system is operational. In this context, it is required that the application and deployment architecture should provide for Scale-Up and Scale out on the Application and Web Servers, Database Servers and all other solution components. The data center infrastructure shall be capable of serving at least 1000 concurrent internal users and 10000 mobile users.

- **Availability** - The architecture components should be redundant and ensure that are no single point of failures in the key solution components. Considering the high sensitivity of the system, design should be in such a way as to be resilient to technology sabotage. To take care of remote failure, the systems need to be configured to mask and recover with minimum outage. The MSI shall make the provision for high availability for all the services of the system. Redundancy has to be considered at the core / data centre 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. MSI must make provisions for security of field equipment as well as protection of the software system from hackers and other threats. Using Firewalls and Intrusion Prevention Systems such attacks and theft should be controlled and well supported (and implemented) with the security policy. The virus and worm attacks should be well defended with gateway level Anti-virus system, along with workstation level Anti-virus mechanism Appropriate insurance cover must be provided to all the equipment supplied under this project. All the system(s) implemented for the Varanasi Smart City Project should be highly secure, with adequate security & protection of the sensitive data relating to the Varanasi City

and its residents. Few such overarching security considerations are briefly described below; the MSI is expected to submit the most appropriate Security Features for the overall ICT Solution:

I. The Generic architecture of smart city generally consists of four layers - a sensing layer, a communication layer, a data layer and an application layer, and these four layers are overseen by the smart city security system. Architecture of information Technology Systems deployed in Smart City need to be open, interoperable and scalable

II. The message exchange between various applications in the smart city should be fully encrypted and authenticated. Any application outside the Data Centre (DC) should talk to the applications hosted in the datacenter through only predefined APls.

III. Convergence of multiple infrastructures into one Central platform for ease of management in a Smart City is mandatory. Applications hosted in the central data center should support multi-tenancy with adequate authentication and Role based access control mechanism for each tenant pertaining to their respective line department infrastructure

IV. The smart city architecture should be capable of managing heterogeneous data, which would be continuously communicated through numerous devices following different protocols. ln order to ensure that the flow of data between devices does not run into latency issues, appropriate protocols need to be deployed so as to minimize latency. The following communication protocols could be used for the different layers for data flow;

- Between applications and back end systems: HTTP, SQL, FTP, SNMP, SOAP, XML, SSH, SMTP

- Between back end systems and field devices: Message Queue Telemetry Transport (MQTT), xMPP, RESTful HTTP, Constrained Application Protocol (CoAP), SNMP, lPv4/6, BACnet, LoNworks, Low Power Wide Area Network (LoRa), Fixed, 4Gl5G, Wi-Fi, WiMax,2Gl3G From field devices: ZigBee olP, ETSI LTN, lPv4/6,6LowPAN, ModBus, Wi-Fi, 802.15.4, enocean, LoRA, RFID, NFC, Bluetooth, DashT" Fixed, ISM & short-range bands.

V. Data Layer (termed as City Digital platform/ fabric) should be capable of communicating with various types of sensors/ devices and their management platforms/applications for

single/multiple services irrespective of software and application they support. Data exchange between various sensors and their management applications must strictly happen through this layer, thus making it one true source of data abstraction, normalization, correlation and enable further analysis on the same. Adequate security checks and mechanisms as described in later points to be deployed to protect data layer from data confidentiality breach and unauthorized access.

VI. The entire information Technology (lT) infrastructure deployed as part of Smart city will follow standards like - ISO 2700'1, ISO 22301, ISO 37120, ISO 3712, ISO 27017, ISO 27018, BSI PAS 180,BSl PAS 18'1, BSI PAS'182, for Wi-Fi access - PEAP (Protected Extensible Authentication Protocol), 3rd Generation Partnership Project (3GPP), etc. or preferably MSI should engage with TPA at the requirement formulation stage for STQC/Cert-in. Cost of the certification will be borne by MSI.

VII. Application Program lnterfaces (APls) should be published and the lT systems be running on standard protocols like JSON / XML or REST etc.

VIII. From a network security perspective all information that flows on the network should be encrypted to ensure safety and privacy of confidential data. The devices at each endpoint of the network should be authenticated (using mechanisms based on attributes one of which could use passwords). The authentication system so used on these endpoint devices should ensure that only authorized users are sending data over the network, and there is no rogue data that is sent to the control systems to generate false alarms or sabotage the systems

IX. All sensors deployed as part of lT and lT based systems in the Smart cities should talk only to the identified Varanasi Smart City network, and do not hook on to the rogue networks' The guidelines to secure wi-fi networks as published by Department of Telecom must be followed

X. Wireless layer of the Smart City Network should be segmented for public and utility networks by using Virtual Private Networks (VPN's) or separate networks in ihe wired core, so that any traffic from the internet users is not routed into the sensor networks and vice-versa.

XI. All traffic from the sensors in the Smart city to the application servers should be encrypted Secure Socket Layer (SSL), PKI and authenticated prior to sending any information. The data at rest and in transit must be encrypted

XII. Authentication of sensors in the Smart city should happen at the time of provisioning lhe sensors, and adding them into the system, and should be based on physical characteristics of the sensors like MAC lD, Device lD etc

XIII. Sensors deployed in solutions to set up Smart city should be hardened devices with the ability to be upgraded remotely for firmware through encrypted image files.

XIV. As various sensors use multiple protocols to communicate with the underlying network with varied security capability, the system should allow provisioning necessary authentication and encryption at the gateway or the nearest data aggregation level if the sensor is not able to do the same.

XV. The Sensors or edge device deployed in Smart city should not have any physical interface for administration. Monitoring of systems and networks should be undertaken remotely.

XVI. All the sensors in the Smart city should connect to an identified network for Varanasi Smart City.

XVII. The data center should be segmented into multiple zones with each zone having a dedicated functionality e.g. all sensors for one operational domain can connect to the data center in one zone, and the internet facing side of the data center should be in another zone

XVIII. The internet facing part of the data center should have a Demilitarized zone where all the customer application servers would be located that are customer facing. Only these servers can access the data from the actual utility application servers on predefined ports

XIX. The customer application servers should be accessed only by the web server that is hosted in a different zone of the data center.

XX. The following should be implemented in the data center - firewalls, intrusion detection & lntrusion prevention systems, Web Application Firewalls, Behavioral analysis systems for anomaly detection, Correlation engine, Denial of Service prevention device, Advanced

Persistent Threat notification mechanism, Federated Identity and access management system, etc.

- Web Proxy Solution:

  Offered solution should be hardened Web Proxy, Caching, Web based Reputation filtering, URL filtering, Antivirus and Anti-malware appliance. All these functionalities should be preferably in a single appliance. Provided operating system should be secured from vulnerabilities and hardened for web proxy and caching functionality.

- Email Security Solution:

  Provided solution should be comprehensive email security solution that integrates against inbound and outbound, Internal defenses against email threat such as spam, virus, etc. Hardware appliance based solution should provide support for anti-spam, anti-virus, outbreak filter, on appliance detail reporting and on- appliance quarantine handling. Appliance should also provision to run Advance malware protection for future requirements.

- NGIPS:

  Solution should include Next Generation Intrusion Prevention System (NGIPS) to provide Advanced Threat Protection solution with future enhancements and protocols. Solution should be for both passive (i.e., monitoring) and inline (i.e., blocking) modes. Detection should be capable of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, zero-day threats, etc.). Solution should also be able to detect threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioral anomaly detection techniques.

XXI. Security lnformation and Event Management (SIEM) monitoring on all Smart City networks, devices and sensors to identify malicious traffic.

XXII. All "applications' and "apps" will undergo static and dynamic security testing before deployment and be tested with respect to security on regular basis at least once in a year'

XXIII. All applications and "Apps" deployed as part of Smart city be hosted in lndia'

XXIV. The said architecture Provide:

- Automatic and secure updates of software and firmware etc.
- All systems and devices should provide auditing and logging capabilities'
- Ensure vendor compliance to remove any backdoors, undocumented and hard cored accounts.
- End-to End solution should be provided with annual end-to-end service availabilily of 99.999 percent. The end to end service agreement should be in place for minimum period of five years form the date of operation. Appropriate teams may be set up to monitor cyber incidents and mitigation of same

XXV. All the information on incidents be shared regularly with lndian Computer Emergency Response Team (CERT-ln) and NCIIPC (National Critical Information infrastructure Protection Centre) and take help to mitigate and recover from the incidents.

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

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

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

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

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

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

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

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

- **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.

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

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

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

- **Interoperability Standards**- Keeping in view the evolving needs of interoperability, especially the possibility that the solution shall become the focal point of delivery of services, and may also involve cross-functionality with the e-Government projects of other departments / businesses in future, the solution should be built on Open Standards. The MSI shall ensure that the application developed is easily integrated with the existing applications. The code does not build a dependency on any proprietary

software, particularly, through the use of proprietary 'stored procedures' belonging to a specific database product. The standards should:

- at least comply with the published e-Governance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and
- be of leading industry standards

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

- Any Passive Networking or Site Preparation/Civil/Electrical work(s) during implementation and O & M period
- Viewing Manpower at the KICCC / viewing centers & Mobile Vans during post-implementation
- FMS staff for non- IT support during post-implementation

However, even if the work is sub-contracted, the sole responsibility of the timely completion of the work & the quality of the work done shall lie with the MSI. The MSI shall be held responsible for any delay/error/non-compliance/penalties/negligence 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 the VSCL and approved by the Competent Authority before any such resource mobilisation.

- **GIS Integration**- MSI shall undertake a detailed assessment for a integration of all the Smart City ICT components with the Geographical Information System (GIS). MSI is required to carry out the seamless integration to ensure ease of use of GIS in the Dashboards in Integrated Command and Control Center (KICCC). If this may require any field surveys, it needs to be carried out by the MSI. Any such data readily available with the VSCL, shall be shared with MSI. However, the MSI is to check the availability of such data and its suitability for achieving the project outcomes. MSI is required to update GIS maps from time to time.

- **SMS Gateway Integration**- MSI shall carry out SMS Gateway Integration with the Smart Varanasi City System and develop necessary applications to send mass SMS to groups/individuals, wherever required. Any external/third party SMS gateway can be used, but this needs to be specified in the Technical Bid proposal, and approved during Bid evaluation. Also, wherever feasible, it is envisaged that the MSI proposes to leverage the existing State Solutions, such as NIC Gateways for this purpose.

- **Application Architecture-** The Applications designed and developed for the Departments concerned must follow the Industry Best Practice(s) and Industry Standard(s). In order to achieve the high level of stability and robustness of the application, the System Development Life Cycle (SLDC) must be carried out using the industry standard best practices and adopting the security constraints for access and control rights. The various modules / application should have a common Exception Manager to handle any kind of exception arising due to internal/ external factors.

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

b) MSI shall design and develop the Smart Varanasi City System as per the study tha would be done by the MSI and as per the scope defined in the RFP

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

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

III. The user of citizen services should be given a choice to interact with the system in local language (Hindi) in addition to English. The application should pave the provision for uniform user experience across the multi lingual functionality covering following aspects:
    - Front end Web Portal in English and 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 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 the local language)

IV. The application(s) should comply with World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG) 2.0 Level AA/Other time to time issued Govt. Of India/Govt. of Uttar Pradesh guidelines for making web content accessible to differently-abled person.

V. 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 auto-populating the forms and dropdowns
- Creation of application form, by "drag & drop" feature using Meta Data Standards
  i. Defining the workflow for the approval of the form
  ii. First in First out
  iii. Defining a Citizen Charter/Delivery of service in a time bound manner
- Creation of the "output" of the service, i.e. Certificate, Order etc.
- Automatic reports
  i. of compliance to citizen charter on delivery of services
  ii. delay reports

VI. 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 Govt. of India / Govt. of Uttar Pradesh. MSI shall ensure using Digital signatures/e-authentication to authenticate approvals of service requests, etc.

VII. e-Transactions & SLA Monitoring Tools

i. The MSI 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 touched through e-Services each day, month and year, through appropriate tools and MIS reports.

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

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

VIII. The Smart Varanasi City Application should have roadmap/capability to integrate with all the key ICT / E-Governance initiatives of the Government of Uttar Pradesh (GoUP) and Govt. of India (GoI), such as Portal Services, Citizen Contact Centres, and Certifying Authorities, etc, as and when required by VSCL.

IX. Complete 'Mobile Enablement' of the 'Smart Varanasi City System'.

C) Other Key Expectations from the MSI

- MSI shall engage early in pro-active consultations with all the Competent Authority, Varanasi City Police and all other key stakeholders to establish a clear and comprehensive project plan, which is in line with the priorities of all project stakeholders and the project objectives.
- MSI will coordinate with the Network Service Provider, shall study the existing fiber layout and existing network in the Varanasi City to understand the existing technology adopted in each of the following areas (not limited to):
- OFC/Network/Wi-Fi
- Surveillance Infrastructure – CCTV Cameras, Data Communication, Monitoring, Control Room and Infrastructure
- Any other Smart City initiatives envisaged for Varanasi
- MSI shall assess existing infrastructure's current ability to support the entire solution and integrate the same with the proposed solution wherever applicable and possible
- MSI shall judiciously evaluate the resources and time planned for undertaking the current state assessment, given the overall timelines and milestones of the project.
- Validate / Assess the re-use of the existing infrastructure if any with Competent Authority site
- Supply, Installation, and Commissioning of entire solution at all the locations
- MSI shall plan the bandwidth required for operationalizing each Smart Varanasi City initiative till the time Competent Authority's own fiber is laid by the MSI as part of the scope of work of this RFP. The bandwidth requirement shall be analyzed and procured by the MSI at its own cost / risk
- MSI shall Install and commission connectivity across all designated locations
- MSI shall establish high availability, reliability and redundancy of the network elements to meet the Service Level requirements
- MSI shall be responsible for planning and design of the access network architecture (access controllers, backhaul connectivity, routers, switches, etc.) to meet the technical, capacity and service requirements for all smart Varanasi City initiatives
- MSI shall be responsible for upgradation, enhancement and provisioning additional supplies of network (including active / passive components), hardware, software, etc. as requisitioned by Competent Authority
- MSI shall ensure that the infrastructure provided under the project shall not have an end of life during the entire contract period.
- MSI shall ensure that the end of support is not reached during the concurrency of the contract and 5 years thereafter
- MSI shall ensure compliance to all mandatory government regulations as amended from time to time

- The MSI shall ensure that all the peripherals, accessories, sub-components required for the functionality and completeness of the solution, including but not limited to devices, equipment, accessories, patch cords (fiber), cables, software, licenses, tools, etc. are provided according to the requirements of the solution
- Competent Authority shall not be responsible if the MSI has not provisioned some components, sub-components, assemblies, sub-assemblies as part of Bill of Materials in the RFP. The MSI shall have to provision these & other similar things to meet the solution requirements at no additional cost and time implications to Competent Authority
- All the software licenses that the MSI proposes shall be perpetual software licenses along with maintenance, upgrades and updates for the currency of the contract. The software licenses shall not be restricted based on location and Competent Authority shall have the flexibility to use the software licenses for other requirements if required
- The MSI shall ensure there is a 24x7 comprehensive onsite support for duration of the contract for respective components to meet SLA requirement. The MSI shall ensure that all the OEMs have an understanding of the service levels required by Competent Authority. MSI is required to provide the necessary MAF (Manufacturer Authorization Form) as per the format provided in the RFP in support of OEMs active support in the project
- Considering the criticality of the infrastructure, MSI 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 system uptime requirements
- MSI shall be responsible for periodic updates & upgrades of all equipment, cabling and connectivity provided at all locations during the contract period
- MSI shall be responsible for setting up / building / renovating the necessary physical infrastructure including provisioning for network, power, rack, etc. at all the locations
- MSI is expected to provide following services, including but not limited to:
    i. Provisioning hardware and network components of the solution, in line with the proposed Competent Authority's requirements
    ii. Size and propose 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 smart Varanasi City 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 Varanasi City Wi-Fi, Varanasi City Kiosk, 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 items
viii. All equipment proposed as part of this RFP shall be rack mountable
ix. Competent Authority may at its sole discretion evaluate the hardware sizing document proposed by the MSI. The. MSI needs to provide necessary explanation for sizing to the Competent Authority
x. Complete hardware sizing for the complete scope with provision for upgrade
xi. Specifying the number and configuration of the racks (size, power, etc.) that shall be required at all the locations.
xii. The MSI shall provide for all required features like support for multiple routing protocols, congestion management mechanisms and Quality of Service support
xiii. The MSI 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. SPECIFIC SCOPE OF SERVICES

4.1 Kashi Integrated Command Control Center (KICCC)

The KICCC shall be created at a location designated and decided by the Competent Authority. The KICCC shall provide a comprehensive system for planning, optimizing resources and response pertaining to the standard functions of the concerned authorities. With a view of enabling varied and respective stakeholders to operate specified Smart City Components, it is proposed to build an Operation Center, housed inside the KICCC, which will cater to the City operations, City Surveillance and Helpdesk in an integrated manner.

With respect to the City Surveillance aspect**,** there shall be a viewing and controlling mechanism for the selected field locations in a fully automated environment for optimized monitoring, regulation and enforcement of services. The KICCC shall be accessible by the operators and concerned authorized entities with necessary authentication credentials. The KICCC shall be used and manned by the designated officials/personnel/staff authorized by the respective Depts. Such as the City Police, Traffic Police and Municipal Corporation, etc. to keep surveillance on civil issues and monitor all civic, PAN City operations.

Competent Authority shall review and carry out a detailed assessment of the proposed design solution and review design for the KICCC and its Data center (DC) on the parameters of overall Design, Safety & Security and reserves the right to accept, reject or suggest for modifications on the proposed solution. The video feed from the surveillance cameras shall be received at the KICCC, where a video wall shall be installed for viewing 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.

With the vision of the fully Integrated City Wide Operations, the Operations Centre of the KICCC shall have the capability to use the 'Internet of Everything' (IoE) Platform w.r.t to all Civic amenities.

In the Varanasi City, various Government agencies provide multiple services to the citizens. With increasing Urbanization, operational challenges are increasing, which in turn affect the quality of services offered to the citizens. These agencies, which often function in silos can provide a wealth of information, which can be utilized for efficient service delivery across the City and facilitate in making decisions anticipating the probable problems and by ensuring cross-agency responsive actions to the issues with faster turnaround time.

The **'Data Center' (DC) infrastructure catering to all the Components & features of the Varanasi Smart City – ICT Solutions, will be co-housed in the KICCC building itself, for which the VSCL will provide the MSI with requisite space and electric power depending on the requirement as per the proposed solution of MSI (Nagar Nigam building which has been identified tentatively as a proposed site for KICCC).** The MSI shall be required to undertake a detailed assessment of the requirements at the KICCC and commission all the necessary ICT and non-ICT infrastructure and also carry out the civil/ electrical work as required. The Data and Surveillance Network can/may share the same physical infrastructure with guaranteed bandwidth for each individual segment. The software components shall provide for a comfortable monitoring experience, easy extraction of clips, and management of storage.

It is envisaged that the IoE Platform shall leverage the information provided by different devices/ platforms & various Departments and providing a comprehensive response mechanism for the day-to-day challenges across the City. The proposed IoE platform shall be a fully integrated portal-based solution that can provide seamless incident – response management, collaboration and geo-spatial display. IoE shall provide real-time communication, collaboration and constructive decision making amongst different agencies by envisaging potential threats, challenges and facilitating effective response mechanisms. Thus, the Integrated Operation Platform (IoE) provides a Common Operating Picture (COP) of various events in real-time on a unified

platform with the means to make collaborative and consultative decisions, anticipate problems to resolve them proactively, and coordinate resources to operate effectively. The IoE platform is envisioned to provide a high processing power and adequate data storage with a high performance information highway to provide process information in real time and serving decision support system. The IoE platform should also provide portability to meet changing Varanasi City scenario. The MSI is required to provision data storage and processing power of the platform adequately to meet the system design and functionality to be achieved**.**

IoE solution should be capable of seamless integration with various government and emergency services such as law enforcement, disaster and emergency services, utility services etc., the proposed solution should support recording of external mobile video feeds, data communication, telephony etc., it should support scenario reconstruction and analytics capabilities with event timelines. The solution should support event logs including operator's onscreen activities, voice & video events, etc. for further analysis, training and similar activities. Built in analytical tools are expected to provide real-time analysis of individual events and also a measure of the incidents for each of the silos integrated on the platform. These are intended to help the decision makers with immediate responsive actions to mitigate / control multiple complex challenges.

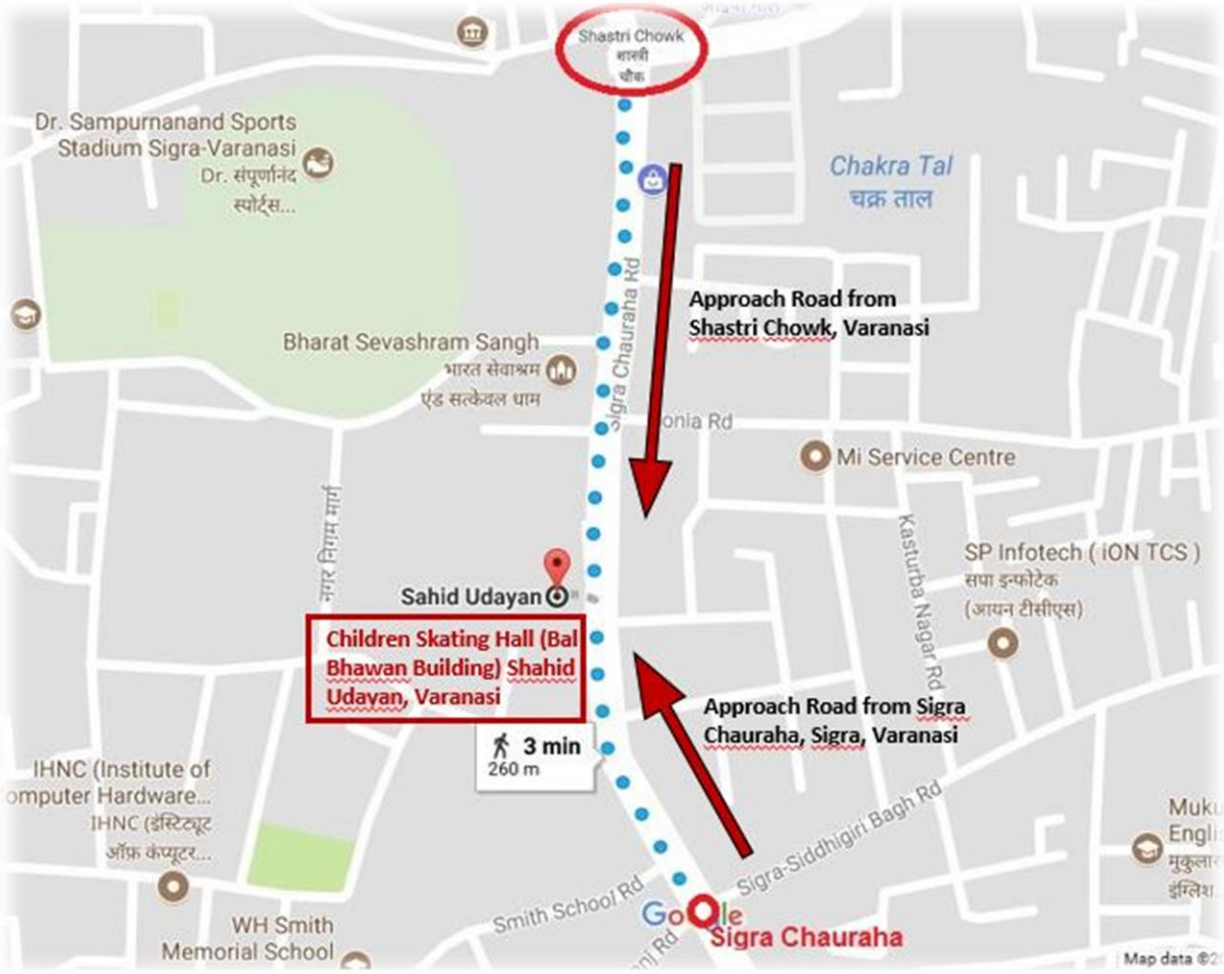
The Varanasi Integrated Smart Solution's platform shall support & have the ability for adding more/new layers of solutions seamlessly with minimal effort as and when required, as and when intended by the Competent Authority intends to develop in time to come such as Water Management, Smart Health, Smart Education & Disaster Management.

The proposed information will be shareable on intra Varanasi City and inter cities levels based on approved rights on mutual consent. On the Integrated Operation Platform (IOE), the system shall provide Standard Operating Procedures (SOPs), step-by-step instructions based on the policies of the Competent Authority and tools to resolve the situation and presents the relevant situation information in a quick and easily digestible format for an operator to verify the situation. The system shall provide reporting & audit trail functionalities to track all the information and monitor operator interactions with the system and to impart necessary training to the users

The Operation Center of the KICCC will have provisions for monitoring and control of all the Smart City Components including the PAN City Surveillance. However, the Competent Authority intends to provision for Varanasi City surveillance monitoring cum viewing for critical field cameras and other security equipment as per the Varanasi City's requirement. Moreover, all this will integrate into IoE platform. The inputs/feeds from the different components of Smart Varanasi City Solutions shall be received at Operation Center video wall for monitoring, tracking and decision support purpose on real time basis supported with GIS

technology. Further, operators shall be working on their respective monitors for assessing the inputs and triggering actions at ground level.

Roadmap to approach proposed KICCC Building



Types of Operations:

A. Normal Operation

Normal operation is when the services function as per pre-planned operation schedule or methodology. Under normal operating conditions various members of Operations team shall coordinate their activities and exchange information through voice and data communications systems about the equipment / facilities under their supervision to facilitate a safe and secure arrangement throughout the entire Varanasi City. Under the normal condition, the operations team shall continuously supervise the main assets and identify any fault, anywhere in system promptly. Operation team shall isolate faulty element and operate the system in a manner to arrange alternatives wherever appropriate alternative is possible (element redundancy, rerouting of services, alternate feeding path etc.). Faulty elements are further referred to appropriate team for respective corrective action. The KICCC Framework shall enable faster isolation of faulty elements & identification & implementation of inbuilt alternatives in system.

B. Degraded Operation

Degraded modes of operation occur when certain systems fail to meet the levels of service that is expected of it. In such scenario the applicable Standard Operating Procedure (SOP) would be followed.

For example: Various failures in power installation may affect the distribution of power in various sectors of the Varanasi City. Load shedding need to be planned looking at many aspects, one of the few could be: Student Exams, Hospitals and Industries.

C. Emergency Operation

In a Smart City, the emergency situations, need to be averted beforehand. Emergency operations are enforced in case of an unforeseen or abnormal situation, when it's not possible to carry on the services. An emergency or disaster is a sudden or great calamity leading to deep distress affecting men and machinery. Many of the accidents / incidents like an act of vandalism, terrorist attack, an accidental fire, critical system failure, force majeure, etc. may lead to crisis / disaster. In cases of disasters, the main objective is to disperse the affected persons, as early as possible, from the affected site of occurrence and avoid loss of life and properties. Management of such situation requires sharing of clear and accurate information and necessary actions shall be initiated without any delay to ensure the restoration of normalcy.

- This requires seamless & timely sharing of information amongst multi-disciplines (viz. Traffic, Parking, Helplines, Smart Lights, Signal & Telecommunication, etc.) involved in Operations and
- Necessitates that appropriate actions are initiated without any delay and the situation is tackled in the most appropriate and efficient manner, so that distress is relieved expeditiously.

Thus, for effective management of such scenarios, it is preferable to have visibility and ability to manage critical disciplines at one place. The KICCC framework shall support Automation of Disaster Management Procedure. The CCTV Cameras throughout the Varanasi City and analytical tools would perform the emergency operations ONLY during this situation.

Site preparation for Kashi Integrated Command & Control Center including Data Center and Helpdesk

The detailed design in all aspects for the design-build (including but not limited to civil, mechanical, structural, electrical, communications, fire, fit-outs, furniture, etc.) of the KICCC shall be the responsibility of the MSI and be approved by the Client or its representative. All interior works of KICCC shall be modular in nature allowing expansions. The MSI may have the required personnel on the team including architect, structural engineer, MEP (Mechanical, Electrical, Plumbing) etc. if needed for this design-build. At least two (2) options for the design-build shall be proposed for the KICCC. Interior layouts and material to be procured for the KICCC shall be approved by the Client or its representative. Preparation includes Kashi Integrated Command and Control Center (KICCC), Data center & Helpdesk. Maintenance of all the infrastructure will be part of Operations & Maintenance till end of contract.

The following is an illustrative diagram of Kashi Integrated Command & Control Center. MSI may suggest better design and get the approval from VSCL.

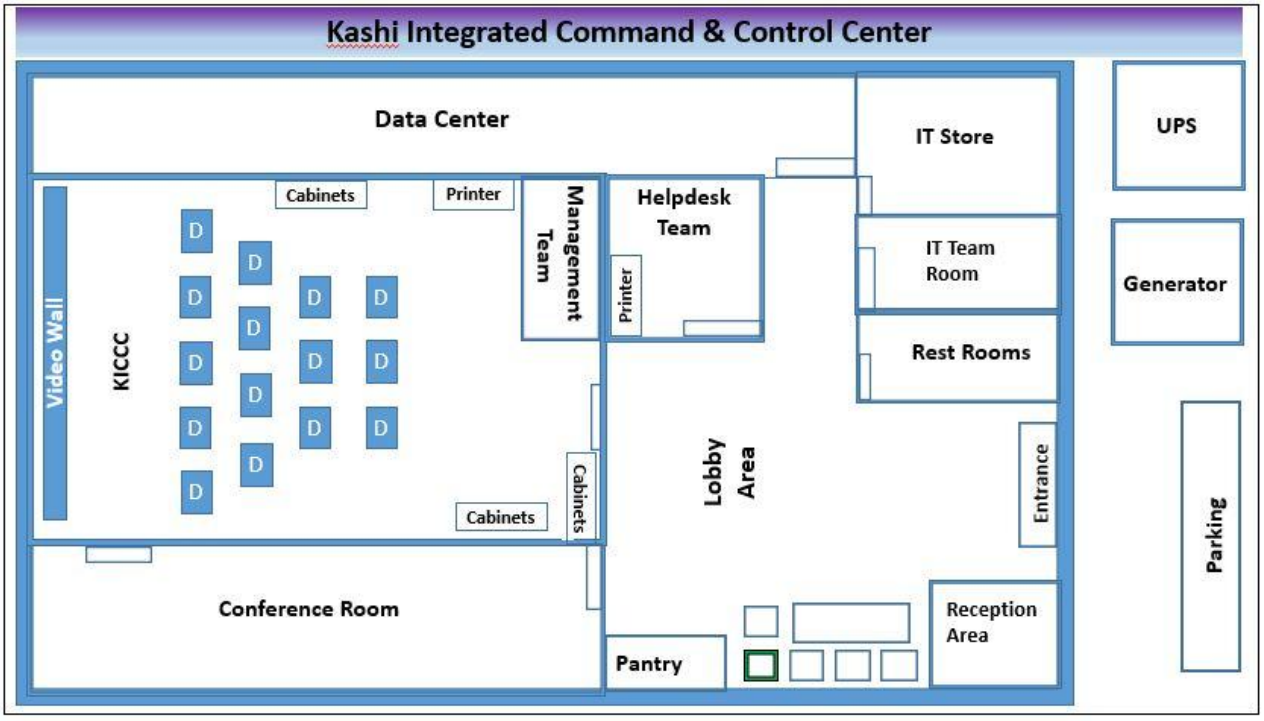


Figure: Illustrative Architecture of Kashi Integrated Command & Control Centre

Norms

The KICCC interiors shall be state of the art adhering to the various best practices norms for control centres, including:

1. Development of ergonomic reports for the KICCC covering Human Factors Engineering (HFE), ISO9241 (Ergonomic requirements for office work with visual display terminals - VDTs) and ISO11064 (Ergonomic Design of Control Centres)
2. The proposed interior material should meet to basic control room norms, including but not limited to:
    - ASTM E84 or equivalent fire norms.
    - High scratch resistant surfaces.
    - Varanasi seismic zone (Zone 3) compliance.
    - Green Guard certified Desks for ensuring safe environment for operators.

The MSI shall be responsible for complete site preparation, installation and commissioning for Kashi Integrated Command and Control Center (KICCC), Data center and Helpdesk as per the requirement in consultation with the Competent Authority but not limited to the following:

Civil and Architectural work

The scope for civil work in this RFP is to furnish the Kashi Integrated Command and Control Center (KICCC), Data center, in all aspects. The furnishing includes but not limited to the following:

1. Cutting and chipping of existing floors
2. Trench works
3. Masonry works
4. Hardware and metals
5. Glazing
6. Paint work
7. False flooring
8. False ceiling
9. Storage
10. Portioning
11. Doors and locks
12. Painting
13. Fire proofing all surfaces
14. Cement concrete works
15. Insulation

All material to be used shall be of fine quality ISI marked unless otherwise specified. MSI is responsible for quality of the civil infrastructure and should take care there is no water leakage in the work.

False Ceiling

The MSI shall install the top false ceiling with 1' 6" of space from the actual room ceiling. This false ceiling shall house A/C ducts (if required) and cables of electrical lighting, firefighting, and CCTV. Appropriate pest control measures shall be taken to keep pests at bay.

Raised flooring

The MSI shall be responsible for raised flooring and provide for suitable pedestal and under structure designed to withstand various static and rolling loads subjected to it in server racks. The entire raised floor shall have laminated floor covering and beadings on all sides of the panel.

Electrical Distribution System

The MSI shall be responsible for proper and uninterrupted working and shall ensure this by having the power distribution system with redundancy:

1. Two incoming HT feeder supply from different sub-stations. Even if one feeder is down, the other one keeps power available.
2. Emergency Diesel- Generator backup on failure of both main feeders.
3. UPS system with battery bank for critical loads.
4. Connection between UPS system and the network switch racks shall be redundant. No single point of failure shall exist in the power connectivity between network racks and UPS system.

Electrical work

The electrical cabling work shall include but not limited to the following:

1. Main electrical panels
2. Power cabling
3. UPS distribution board
4. UPS point wiring
5. Power cabling for utility component and utility points etc.
6. Online UPS
7. Separate Earth pits for the component
8. The MSI shall use fire retardant cables of rated capacity exceeding the power requirements of existing and proposed components to be used at maximum capacity.
9. All materials to conform to IS standards as per industry practice

Lighting Works

MSI shall be responsible for the lighting works in the facility. Following items need to be undertaken by MSI for lighting:

1. Supply of all equipment associated with implementation of lighting including fixtures, lamps, wiring etc.
2. Wiring for lighting system in the building
3. Installation of lighting fixtures
4. Warranty for the lighting equipment
5. Critical lights shall be connected to UPS for uninterrupted lighting

6. Post the installation, MSI shall ensure that lux levels of the building are as per IES-HB-10-11 and requirements of this RFP.

UPS requirements and features

UPS system shall provide a redundant power supply to the following needs:

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

The system shall be automatic with power supply from the mains and automatic switchover to DG set as secondary source.

Diesel Generator Set

The diesel generator set shall be in N+1 redundancy mode where N = 1. MSI has to specify the technical specifications based on the requirement. The MSI shall be responsible for regular operations and maintenance of the DG set. The MSI shall be responsible for but not limited to:

1. Fuel
2. Preventive maintenance
3. Corrective maintenance
4. AMC, if any
5. Replacement of any parts etc.

Air Conditioning and Natural Convection

Since KICCC and Data Center are quite critical areas, precision air conditioning system shall be exclusively installed to maintain the required temperature. The A/C shall be capable of providing sensible cooling capacities at ambient temperature and humidity with adequate air flow. The task of the MSI shall include (but not limited to):

1. Connecting the indoor unit with the mains electrical point
2. Connecting indoor and outdoor units mechanically (with 18 G hard gauge copper piping)
3. Connecting indoor and outdoor unit electrically

The air conditioner shall be linked to secondary power supply as well to prevent them from shutting down in case of power outage.

Fire Detection and Suppression System

The facility shall be equipped with adequate and advanced Fire Detection and Suppression system. The system shall raise an alarm in the event of smoke detection. The system shall have proper signage, response indicators and hooters in case of an emergency. The system shall be based as per NFPA standards. The facility is to be equipped with gas based (Suitable for Data center environments) fire suppression system appropriately sized for the given size of the Data center and KICCC.

Building Management System

1. Building Management System shall be implemented for effective monitoring, management, control and integration of various building systems such as HVAC, lighting, electrical, fire detection and suppression system, CCTV system, Access Control System etc. over a single platform. BMS shall perform various functions such as data collection and archival, alarm and event management, trending, reports and MIS generation, preventive maintenance etc.
2. Design-Build of the BMS shall be under the scope of MSI. IO summary and other BMS related provisions shall fall under the scope of the MSI.

Access Control System

The Biometric/Access card based Access Control System shall be deployed with the objective of allowing entry and exit to and from the premises to authorized personnel only with appropriate door locks and controller assemble connected with BMS system. The system deployed shall be based on proximity as well as biometric technology for critical areas and proximity technology for non-critical areas.

CCTV system

The MSI shall provide CCTV system within the Data center and KICCC on 24X7 bases. All important areas of the Data center, KICCC along with the non-critical areas like locations for DG sets, entry exit of Kashi Integrated Command Control Center (KICCC), Entry and Exit of building premises need to be under constant video surveillance. Monitoring cameras shall be installed strategically to cover all the critical areas of all the respective locations.

Water leak detection system

The Water Leak Detection System shall be installed to detect any seepage of water into the critical area and alert the security control room for such leakage. It shall consist of water leak detection cable and alarm module. The cable shall be installed in the ceiling and floor areas around the periphery.

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, the MSI shall conduct periodic pest control using chemical spray once in a quarter as a contingency measure to effectively fight pests.

KPIs for KICCC:

1. The vision of the Kashi Integrated Command and Control Center (KICCC) 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. Integrated Command and Control Center involves leveraging on the information provided by various departments and providing a comprehensive response mechanism for the day-to-day challenges across the city. KICCC shall be a fully integrated, web-based solution that provides seamless incident – response management, collaboration and geo-spatial display.
3. KICCC 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. KICCC will provide 24*7 City Surveillance System for effective management of the city.
6. KICCC shall leverage state of the art technology to effectively manage Road Traffic and
7. KICCC should be able to integrate with various Utility systems such as Water/SCADA, Power, Gas, ITMS, Sewerage/ Drainage system, Disaster Mgmt. System etc.

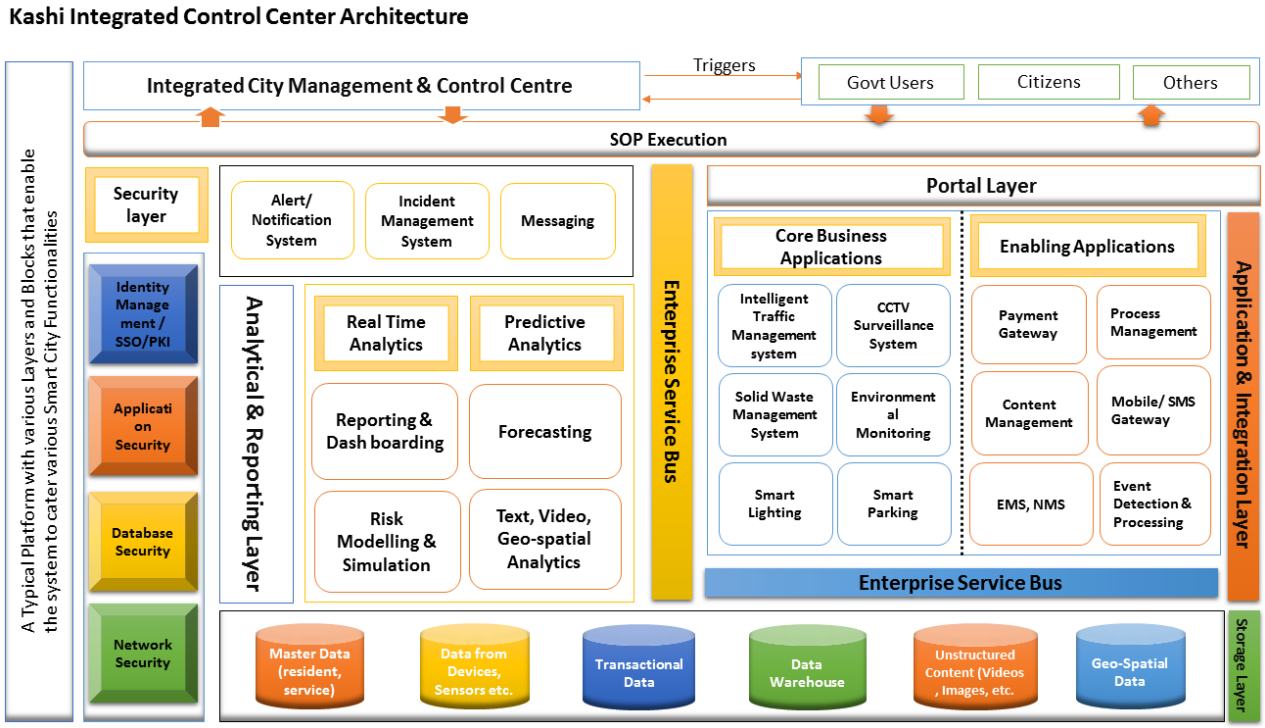


Figure: Illustrative Layered Architecture of Kashi Integrated Command & Control Centre

Functional Specifications for KICCC:

Proposed components/requirements of Integrated Command and Control Centre for Varanasi city:

1. Integrated Command and Control Application.
2. Unified Communications and Contact Centre.
3. Integrated Dashboard- ITMS, City Surveillance, SWM, Smart Parking, etc.
4. Video Wall & Controller System.
5. Operator Workstation and Accessories.
6. Alerting System.
7. Integration with Third Party Shared Services.
8. Helpdesk Service, Women and Elderly Helpdesk
9. Necessary Civil, Electrical work including furniture, including Air-conditioning for Data Centre, and Command & Control Centre.

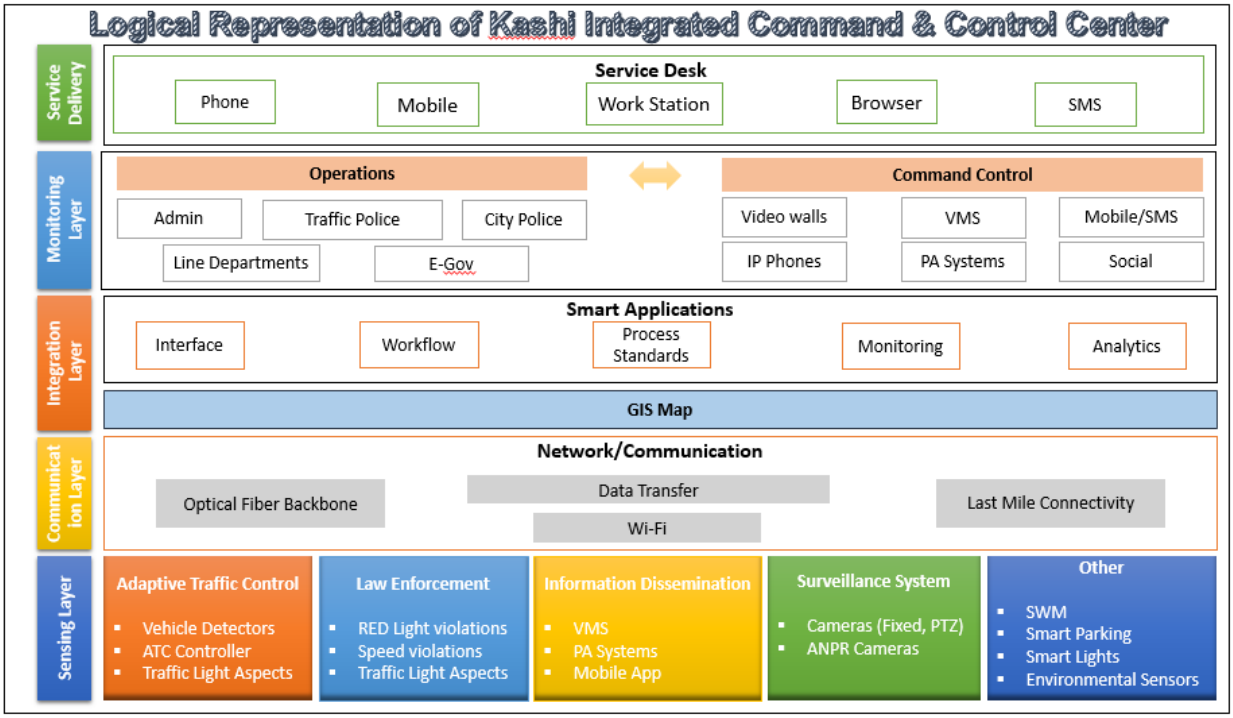


Figure : Illustrative Logical Representation of Kashi Integrated Command & Control Center

Integrated Command and Control Centre System

Sr. No.	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. ▪ 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. ▪ 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.) ▪ System must provide a comprehensive API (Application Programming Interface) or SDK Software Development Kit) to allow interfacing and integration with existing systems. ▪ Software (Application, Database and any other) must not be restricted by the license terms of the OEM from scaling out

Sr. No.	Functions	Minimum Specifications
		on unlimited number of cores and servers for future expansion. ▪ 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 ▪ The platform should be able to integrate with any type of sensor platform being used for the urban services irrespective of the technology used. Must have built-in fault tolerance, load balancing and high availability & must be certified by the OEM. ▪ Platform should support on the fly deployment of Sensors. Platform shall have the ability to add / remove sensors including new vendor types without a need for shutdown. ▪ Platform should support Cross collaboration APIs thereby enabling contextual information and correlation across domains and verticals.
2	**Command and Control Center Components**	▪ Web Server to manage client requests. Client/User should be provided with web-based, one-stop portals to event information, overall status, and details. ▪ The User Interface (UI) to present customized information in various preconfigured views in common formats. All information to be displayed through easy-to-use dashboards. ▪ Application Server to provide a set of services for accessing and visualizing data. Should be able to import data from disparate external sources, such as databases and files. It should provide the contacts and instant messaging service to enable effective, real-time communication. It should provide business monitoring service to monitor incoming data records to generate key performance indicators. It should also provide the users to view key performance indicators, standard operating procedures, notifications, and reports, spatial-temporal data on a geospatial map, or view specific details that

Sr. No.	Functions	Minimum Specifications
		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
3	**Industry Standards for the Command and Control Center**	▪ The solution should adhere to the industry standards for interoperability, data representation & exchange, aggregation, virtualization and flexibility. IT Infrastructure Library (ITIL) V3 or above standards for Standard Operations Plan & Resource Management ▪ Geo Spatial Standards like GML & KML etc. ▪ Business Process Model and Notation (BPMN) or equivalent for KPI Monitoring.
4	**Availability, Scalability, Performance and Usability**	• The KICCC system shall be highly available platform. • The system shall be very tolerant to losses or reduction of communication such that the system shall recover gracefully from such incidents, with no human interaction required. • Should have a high performance and high availability architecture. • Shall be flexible, modular and tolerant to failures/errors and able to exchange information with other systems • The system must have an open architecture such that additional systems when added can be integrated with CCA without upgrades or disruption to other interfaces. • The communications use standard components that are widely available. Should allow scalability and flexibility to include more applications / solutions in the future • The KICCC server shall refresh system GUI within 1 second of an incident trigger requiring a change of state in the information in the database. • The KICCC server hardware shall be based on high

Sr. No.	Functions	Minimum Specifications
		availability, fault tolerant design and capable of operating in mirrored server configuration. The KICCC system shall have a resilient processing architecture such that failure of a single component does not affect entire KICCC application. • The system shall be able to operate at network bandwidth down to a minimum of 1 mbps. • The system shall be able to operate at network latencies as long as 2 seconds.
5	**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 the city (being implemented as part of this project or other projects) to create actionable intelligence
6	**Integrated User Specific & Customizable Dashboard**	• Should provide integrated dashboard with an easy to navigate user interface for managing profiles, groups, message templates, communications, tracking receipts and compliance Collects major information from other integrated City sensors/platforms. • Should allow different inputs beyond cameras, such as, User desktop screens, web page, and other external devices for rich screen layout • Multi-displays configurations • Support for GIS tool which allows easy map editing for wide area monitoring (Google map, Bing map, ESRI Arc GIS map, etc.). • Should provide tools to assemble personalized dashboard views of information pertinent to incidents, emergencies & operations of command centre • Should provide dashboard filtering capabilities that enable

Sr. No.	Functions	Minimum Specifications
		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 Should provide historical reports, event data & activity log. The reports can be exported to PDF or HTML formats.
7	**Authentication & Encryption**	• Use authentication information to authenticate individuals and/or assign roles. • Support LDAP authentication mechanism • Support for PKI implementation
8	**Flexible Single Sign-On (SSO)**	SSO to Web-based applications that can span multiple sites or domains with a range of SSO options.
9	**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.
10	**Internet Security**	Provide comprehensive protection of web content and applications on back-end application servers, by performing authentication, credential creation and authorization.
11	**API Integration**	Platform OEM should have published the normalized APIs in their website for the listed domains ((Parking, Outdoor Lighting, Traffic, Environment, Urban mobility etc.) to allow sensor vendors and app developers to develop their connectors / adaptors to the platform
12	**API Security**	• The access to data should be highly secure and efficient. • Access to the platform API(s) should be secured using API keys. • Software should support security standards: OAuth 2.0, HTTPS over SSL, and key management help protect the data across all domains. • Should support security features built for many of its components by using HTTPS, TLS for all its public facing API implementations. For deployment where CCC Software API(s) exposed to application eco system, API Management, API security features and API Key management functions are required.

Sr. No.	Functions	Minimum Specifications
13	**Developer Tools**	KICCC platform should provide online Developer tools that help City to produce new applications, and/or use solution APIs to enhance or manage existing solution free of cost. Platform should have an online public facing web interface and support should be available 24X7.
14	**Service management**	Data brokerage, ID Management: Performs service management
15	**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.
16	**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
17	**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.
18	**Rule Engine & Optimization**	• Should have ability to respond to real-time data with intelligent & automated decisions • Should provide an environment for designing, developing, and deploying business rule applications and event applications. • The ability to deal with change in operational systems is directly related to the decisions that operators are able to make. • Should have at-least two complementary decision management strategies: business rules and event rules. • Should provide an integrated development environment to develop the Object Model (OM) which defines the elements and relationships
19	**Remote Video Display**	• The system should support dynamic reduction of bit rate and bandwidth for each stream based on the viewing resolution at the remote location. (Example: If the remote station is viewing with 352 x 240 (CIF), the stream to remote viewing location should not be using HD bandwidth, but dynamically should

Sr. No.	Functions	Minimum Specifications
		change to lower bandwidth. If the remote viewing station is viewing this camera in full screen 1080P, then it should dynamically increase the bandwidth to provide HD experience.) • The system should use dynamic channel coverage specifically for video stream function for efficient bandwidth usage for multiple operation center and only transmits video stream required to display on monitor to maximize bandwidth efficiency and should support 20 to 30 camera feeds in single display. • The solution should comprise of video processing server. This server must be able to carter to following functional requirements: a) To process and transmit video streams adaptive to each video requests to optimize network bandwidth usage. b) Shall be able to distribute real-time video streams without any loss in original video quality
20	**Device Engine**	• Aggregation and abstraction of sensors: provides aggregation of sensors from diverse sensor cloud • Normalization of sensor data: organizes sensor data and assigns attributes based on relations; raw data removed and passed to data engine
21	**Location Engine**	• Map services and geospatial coordinates: provides the geographical coordinates of specific facilities, roads, and city infrastructure assets, as well as unmapped facilities • Geospatial calculation: calculates distance between two, or more, locations on the map • Location-based tracking: locates and traces devices on the map
22	**Enterprise Resource Planning (ERP) Integration capabilities**	System should allow integration of business process in ERP workflows like property, water tax collection etc.
23	**Data Engine**	Data archive and logging: stores data feeds from the device engine and external data sources

Sr. No.	Functions	Minimum Specifications
24	**Incident Management Requirements**	• Should provide facility to capture critical information such as location, name, status, time of the incident and be modifiable in real time by multiple authors with role associated permissions (read, write). • Incidents should be captured in standard formats to facilitate incident correlation and reporting. • The system must provide Incident Management Services to facilitate the management of response and recovery operations • Should support comprehensive reporting on event status in real time manually or automatically by a sensor/CCTV video feeds. • Should support for multiple incidents with both segregated and/or overlapping management and response teams. • Should support for sudden critical events and linkage to standard operating procedures automatically without human intervention. • The system must identify and track status of critical infrastructure / resources and provide a status overview of facilities and systems • Should support plotting of area of impact using polynomial lines to divide the area into multiple zones on the GIS maps. • Should support Geospatial rendering of event and incident information. A Reference Section in the tool must be provided for posting, updating and disseminating plans, procedures, checklists and other related information. • Should provide detailed reports and summary views to multiple users based on their roles. • Should support incorporation of resource database for mobilizing the resources for response. • Provide User-defined forms as well as Standard Incident Command Forms for incident management.
25	**Event Correlation**	• ICCC should be able to correlate two or more events coming

Sr. No.	Functions	Minimum Specifications
		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.
26	**Events and Directives control**	Should provide the capability for the events that are produced from a sub- system and are forwarded to the KICCC. 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 KICCC, the event should be displayed on an operations dashboard and analyzed to determine a proper directive. Directives issued by the KICCC 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.
27	**Device Status, Obstruction Detection and Availability Notification**	• Should provide icon based user interface on the GIS map to report non-functional device. • Should also provide a single tabular view to list all devices along with their availability status in real time. • Should provide User Interface to publish messages to multiple devices at the same time
28	**Standard Operations Procedures (SOPs)**	• ICCC should provide for authoring and invoking un-limited number of configurable and customizable standard operating procedures through graphical, easy to use tooling interface. • Standard Operating Procedures should be established, approved sets of actions considered to be the best practices for responding to a situation or carrying out an operation. • The users should be able to edit the SOP, including adding, editing, or deleting the activities. • The users should be able to also add comments to or stop the SOP (prior to completion). • There should be provision for automatically logging the actions, changes, and commentary for the SOP and its

Sr. No.	Functions	Minimum Specifications
		activities, so that an electronic record is available for after-action review. • The SOP Tool should have capability to define the following activity types: ▪ **Manual Activity** - An activity that is done manually by the owner and provide details in the description field. ▪ **Automation Activity** - An activity that initiates and tracks a particular work order and select a predefined work order from the list. ▪ **If-Then-Else Activity** - A conditional activity that allows branching based on specific criteria. Either enter or select values for Then and Else. ▪ **Notification Activity** - An activity that displays a notification window that contains an email template for the activity owner to complete, and then sends an email notification. ▪ **SOP Activity** - An activity that launches another standard operating procedure.
29	**Key Performance Indicator Display**	• ICCC should be able to facilitate measurement or criteria to assay the condition or performance of departmental processes & policies. • Green indicates that the status is acceptable, based on the parameters for that KPI, no action is required. • Yellow indicates that caution or monitoring is required, action may be required. • Red indicates that the status is critical and action is recommended.
30	**What-if Analysis Tool**	• The solution should provide the capability to manage the emergencies and in-turn reducing risks, salvaging resources to minimize damages and recovering the assets that can speed up recovery. • To take proactive decisions that help minimize risks and

Sr. No.	Functions	Minimum Specifications
		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.
31	**Reporting Requirements**	• ICCC should provide easy to use user interfaces for operators such as Click to Action, Charting, Hover and Pop Ups, KPIs, Event Filtering, Drill down capability, Event Capture and User Specific Setup • The solution should generate Customized reports based on the area, sensor type or periodic or any other customer reports as per choice of the administrators
32	**Alarm Display**	• Should have an ability to display alarm condition through visual display and audible tone • Should have an ability to simultaneously handle multiple alarms from multiple workstations • Should have an ability to automatically prioritize and display multiple alarms and status conditions according to pre-defined parameters such as alarm type, location, sensor, severity, etc. • Should display the highest priority alarm and associated data / video in the queue as default, regardless of the arrival sequence.

Sr. No.	Functions	Minimum Specifications
33	**Historical Alarm Handling**	• Should have an ability to view historical alarms details even after the alarm has been acknowledged or closed. • Should have an ability to sort alarms according to date/time, severity, type, and sensor ID or location.
34	**Alarm Reporting**	• Should have an ability to generate a full incident report of the alarm being generated. • Should have an ability to display report on monitor and print report. • Should have details of alarm including severity, time/date, description and location. • Captured video image snapshots. • Relevant sensor data such as SCADA sensors, Response instructions, Alarm activities, (audit trail). • Should have an ability to export alarm report in various formats including pdf, jpeg, html, txt, and mht formats. • Should have an ability to generate an alarm incident package including the full incident report and exported sensor data from the incident in a specific folder location.
35	**Alarm Policies and Business Logic Administration**	• The CCA solution should have the following ability to handle the workflow alarms through graphical user interface. • Should have an ability to match keywords or text from the alarming subsystem's incident description to raise an alarm using criteria including exact match, exact NOT match, contains match, wildcard match and regularly expression match (such as forced door alarm, denied access, door open too long, etc.) • Should have an ability to optionally match alarming subsystem's incident status, incident severity, and sensor type • Should have an ability to apply any alarm policy to one or more monitoring area(s) or zone(s) without having to reapplying the policy multiple times. • Should have an ability to apply any alarm policy to one or more sensors without having to reapply the policy multiple

Sr. No.	Functions	Minimum Specifications
		times. • Should have an ability to assign specific actions for each alarm • Should have an ability to activate or deactivate alarms as required • Should have an ability to create exceptions • Should Create batch-wise rules and process them • Should Check and rectify logical errors and contradictory rules • Should have an ability to schedule execution of rules • Should Suspend or Terminate the application of rule • Should archive unused or deactivated rules
36	**Collaboration Framework/ Tools**	• Shall establish a collaborative framework where input from different functional departments of city municipal corporation and other smart city stakeholders such as transport, water, police, e-governance, etc. can be assimilated and analyzed on a single platform; consequently resulting in aggregated city level information. • This aggregated city level information can be converted to actionable intelligence, which would be propagated to relevant stakeholders and citizens. • Cross collaboration APIs: Enabling contextual information and correlation across domains and verticals (Multiple vendor and Multi-sensor in future). • The KICCC platform` should have the capability to bring in multiple stake holders automatically into a common collaboration platform like persistent chat rooms and virtual meeting rooms in response to a SOP defined to handle a particular event. • The KICCC platform should provide an ability to bring multiple stake holders on to a common voice conference call in response configured events. The stake holders can be on various types of devices like computer, smart phones, tablets or normal phones. • The operator should also have ability to create these

Sr. No.	Functions	Minimum Specifications

		collaboration spaces like virtual meeting rooms or chat groups manually.
		• Shall offer the ability to create graphical displays that are representing real-time conditions in a useful, intuitive format.
		• Shall enable the user to look at various operating areas and see, at a glance,
		  • What's going on?
		  • What are the current problems?
		  • What things are going well?
		  • Do I need to dispatch maintenance/emergency response?
		• Should provide tools for users to collaborate & communicate in real-time using instant messaging features.

37	**Communication Requirements**	• The solution should adhere to the below mentioned communication requirements. • Provide the ability to search/locate resources based on name, department, role, geography, skill etc. for rapidly assembling a team, across department, divisions and agency boundaries during emergency • Provide the capability to invite using information provided during the location of those individuals or roles, invite them to collaborate and to share valuable information. • Provide a single web based dashboard to send notifications to target audiences using multiple communication methods including voice-based notification on PSTN/Cellular, SMS, Voice mail, E- mail and Social Media • The solution should provide Dispatch Console 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 &

Sr. No.	Functions	Minimum Specifications
		dispatch mobile resources available nearby the incident location. Augment resources from multiple agencies for coordinated response.
38	**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.
39	**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. • Provide a single web based dashboard to send notifications to target audiences using multiple communication methods including voice-based notification on PSTN/Cellular, SMS, Pager, Voice mail, E-mail and Social media • 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.
40	**Analytics Engine**	• Analytics Engine should be an artificial intelligence-based smart city analytics platform module to maximize business value through advanced machine learning capabilities. The machine learning capabilities aid in automating policies that result in better asset and infrastructure management. • The solution should be flexible to integrate with other city and government software applications. • Analytics Engine module should have below intelligence capabilities: a) Advanced Predictive Analytics should be part of the

Sr. No.	Functions	Minimum Specifications
		solution. b) The solution should be flexible to integrate with other city and government software applications c) The solution should be able to predict insights consuming data from city infrastructure viz., Traffic, Parking, Lighting etc. d) The solution should have predictions with measurable accuracy of at least > 70% e) The solution should be able to predict and integrate with Smart City solutions helping in driving operational policies creation. f) The solution should be robust, secure and scalable. • The solution should have a visualization platform to view historic analytics The application should enable the customers to discover, compare, and correlate data across heterogeneous data sources to unravel the patterns that are previously hidden. At a broader level, when you work with the application, system do the following tasks: a) Connect to a variety of data sources b) Analyze the result set c) Visualize the results d) Predict outcomes • Analytics Engine should support multiple Data Sources. Min below standard data sources should be supported from day one: a) CSV, TSV, MS Excel , NoSQL, RDBMS • Analytics Engine should provide analysis of data from a selected data source(s). • Analysis enables to define arithmetic and aggregation operations that result in the desired output. • Analytics engine should provide capability to check analysis with multiple predictive algorithms
41	**Analytics Visualizations**	• Analytics Engine should provide visualizations dashboard. • In the visualization workspace it should allow to change visual attributes of a graph. • User should not be allowed to alter the graph/visualization definition. • In the visualizations workspace, user should able to do the following operations: a) Change the graph/visualization type

Sr. No.	Functions	Minimum Specifications
		b) Print the graph c) Export the graph d) Narrow down on the value ranges e) Toggle the axis labels • Integrate with other 3rd party applications seamlessly
42	**Integration with Social Media & Open Source Intelligence**	• Should provide integration of the Incident Management application with the social media. • Should provide analytics based on the social media feed collected from the open source intelligence and collate with the surveillance inputs to alert the responders for immediate action on the ground. • Should provide notifications to multiple agencies and departments (on mobile) that a new intelligence has been gathered through open source/social media. • Should be able to identify the critical information and should be able to link it to an existing SOP or a new SOP should be started. • Should extract messages and display it in an operational dashboard. Should be able to correlate the extracted message from the social media with existing other events and then should be able to initiate an SOP.
43	**Summary Dashboard**	• Shall provide alarm summary of each monitoring zone or monitoring area in graphical chart format • Shall display the following charts per global area, monitoring zone or monitoring area • Shall Open Alert Count by Monitoring Zone/Monitoring Area • Shall have the capability of New vs. Viewed (Opened Alerts) • Shall Open Alert Count by Alert Severity • Should have Highest Severity Alert • Shall enable Monitoring Zone or Monitoring area default to Summary view dashboard or to a map when the zone or area is selected.

Sr. No.	Functions	Minimum Specifications
		• Shall provide a tabular list of sensors in each monitoring.

Video Conferencing System

Video Conferencing System – General Requirements		
Sr. No.	**Component**	**Specifications**
1	**System Features**	Conferencing System should have minimum 24 ports at 1080p 60fps on IP in continuous presence mode with 60fps and H.264 resolution and AES encryption
		Multi-point video Conferencing Solution should be capable of offering a Full High Definition 1080p 60fps in real-time for 24 number of concurrent ports/systems in single call or multiple multi-party sessions in continuous presence and voice activation mode & with intelligent built-in capability for dynamic bandwidth, resolution matching to give each user an experience basis his available bandwidth.
		It should as well provide network flexibility for a reliable distributed architecture and cost-effective scalability for future requirements.
		Conferencing System should be deployed in High Availability and should be redundant (1:1)
		It should have an internal inbuilt hot- swappable redundant power supply.
		It should provide flexibility to the users, where users can join the video conference call using WebRTC compatible browser. This facility should be available from day one.
		The systems should support document sharing (PC images, etc.).
2	**Video Standards and Resolutions**	It should support H.263, H.264, WebRTC. It should support 1080p 60fps, 30 fps, 720p 30 and 60 fps.
3	**Content Standards and Resolutions**	Content sharing should be possible at 1080p 30fps
		It should support H.239 and encryption in SIP & H.323 modes
4	**Audio Standards and Features**	It should support G.711, G.722, G.722.1
		It shall support aspect ratio of 16:9 and 4:3.

		It shall support a mix of resolutions in both Voice-activated mode and Continuous Presence. Each endpoint shall receive at the maximum of its capacity without reducing the capacity of another.
		Dynamic CP layout adjustment (it will choose the best video layout according to the number of participants in the conference).
		It should support distributed architecture with intelligent and automatic call routing. It must support load balancing such that in case there are two instances, conference participants can get distributed across these two instances based on their locations and still join into the same conference.
5	**Network and security features**	It shall support AES encryption 128 bit or above for every participant without affecting any other feature, functionality or port count.
6	**Interoperability**	Apart from Integrated video systems, video IP phones, normal IP phones also should be able to join the conference seamlessly
7	**General Standards**	Should be based on ITU's (International Telecommunication Union) standards and guidelines.
Management & Scheduling		
Sr. No.	**Component**	**Specifications**
8	**System**	The central management solution should be able to schedule the meeting quickly and easily manage conference infrastructure device configuration and provision of the endpoints.
9	**System Capacity**	The Central management server must support 10 devices capacity from day one and must be scalable.
10	**Provisioning**	The administration should be able to configure individual end points or group of endpoints using user policy from single management console.
		It should be possible for the endpoint to automatically pull the device and site provisioning information from the system while start up
11	**Software Update**	It should be capable of automatic and scheduled mechanism to upgrade the software on one or more endpoints with a standard software Work thereby eliminating the need to upgrade each 6 endpoint individually.
12	**Scheduling**	The system should support schedule video conference meetings.
13	**Directory Services**	Should support integration with the corporate Active Directory for scheduling the video conference calls.

		The system should store video dialling information.
Voice and Video Call Control		
Sr. No.	**Component**	**Specifications**
14	**System**	The Call control solution should be able to register Integrated VC room system, Video IP phones, normal IP phones natively.
		The system should be a converged communication System with ability to run TDM and IP on the same platform using same software load based on server and Gateway architecture
		It should be possible to deploy Servers / Call Servers in an active-active configuration over the distributed IP infrastructure (LAN/WAN). The call control system should be fully redundant solution with no single point of failure & should provide 1:1 redundancy. Both the servers should do call processing all the time and act as backup in case of the failure of one server
		The communication feature server and gateway should support IP V6 from day one so as to be future proof
		The offered solution must provide a standard based mechanism for QoS implementation
		Should support AD & LDAP integration for directory synchronization & user authentication
15	**Support for call-processing and call-control**	Should support signalling standards/Protocols – SIP, MGCP, H.323, Q.Sig
		Voice Codec support - G.711, G.729, G.729ab, g.722, ILBC. Video codecs: H.261, H.263, H.264, and Wideband Video Codec
		Video telephony support
		System should be supplied with 50 endpoint license
16	**Security**	The protection of signalling connections over IP by means of authentication, Integrity and encryption should be carried out using TLS
		System should support MLPP feature
		Proposed system should support SRTP for media encryption and signaling encryption by TLS
		Secure HTTP support for Call Server Administration, Serviceability, User Pages, and Call Detail Record Analysis and Reporting Tool.

		Should support Secure Sockets Layer (SSL) for directory
Fully Integrated Single Room System		
Sr. No.	**Component**	**Specifications**
18	**Protocols**	Should support H.320 (ISDN Video conferencing) as well as H.323 (LAN Video Conferencing) standards. The system should be able to call any H.323 and SIP endpoint directly or indirectly.
		It should be possible to share content via BFCP and H.239
		Endpoint should support the latest video coding standard eitherH.263, H.264, H.265
		It should support Audio coding G.722, G.722.1, G.711
19	**Network**	Endpoint should support bit rate up to 8 Mbps or more on IP (H.323and SIP)
		Minimum 2 X Gigabit Ethernet: Should support 10/100/1000 BASET
20	**Main Video Resolution**	Shall work in high definition video resolution of 1080p 60fps for live video for both Transmit and receive
21	**Camera**	Inbuilt in the Integrated system with 2 cameras
		Both cameras should be capable of automatic voice tracking capability so as to automatically zoom and focus on to the person speaking in the room.
		Zoom: Minimum 10x (optical) or better
22	**Video Inputs**	Minimum 3 HDMI inputs and 1 DVI input for connecting PC / laptop
23	**Video Outputs**	Minimum 2 x HDMI or similar or better to connect two displays. Additional Outputs are desirable. It should support minimum 7
24	**Audio Inputs**	Omnidirectional / Directional Microphones. 3 microphones to be supplied from day one with the system.
25	**Encryption**	AES 128 bit or more, TLS, SRTP, HTTPS or similar or better
26	**User Interface**	Intuitive touch panel to operate the entire system
Video device with minimum 22-inch screen		
Sr. No.	**Component**	**Specifications**

27	**System**	Should be an integrated system with at least 14-inch LCD/TFT screen, 1080P resolution (16:9), HD camera and with speakers for wideband audio output. The Codec should be a part of the unit. No separate codec and Screens must be used
		The LCD/TFT screen should be a touch screen to provide a touch interface to the user
		Video Standards:
		• Minimum H.264 and above
		• The system should support SIP protocol
		• Must support desktop sharing SIP calls
		Video Frame Rate: Must support 1080p 30 fps
		Video Input: Should have HDMI or DVI (Digital Video Interface) input to connect PC/Laptop directly to the Video conferencing system and display a resolution of XGA/SXGA. The user must be able to toggle between the Laptop/PC mode and the Video conferencing mode at a push of button/icon.
		Video Output: Must have an HD output via an HDMI/DVI output port to display the VC screen onto an external display
		Should have inbuilt microphone & speaker system.
28	**Security**	Security - Password protected system menu
29	**Camera**	Should be HD at least 6-megapixel camera, with privacy shutter
		Must support 1080p resolution. Should support Wide formats. Must support 1920 X 1080 resolution
		The VC unit must allow the camera to be used as a document camera to capture hard copies and transmit it to the far end site

Integration Capabilities

Sr. No.	List of Services	Brief of Scope for Integration
1	**Integration of Intelligent Traffic Management System (Police)**	• KICCC will be required to integrate with Command Center of Traffic Management System, to receive real-time feeds of the camera installed by them. • These video feeds will not be saved, but will be utilized in Analytical layer to help administration monitor its assets and do a better urban planning.

Sr. No.	List of Services	Brief of Scope for Integration
		• KICCC will also be required to send video feeds received from Smart Parking, Smart Pole, PBS in real-time basis to the command center of Traffic (if required). KICCC should also be able to trigger the commands / alerts (if required) to the respective command center.
2	**Integration with CCTV Surveillance (Police Dep't.)**	• KICCC will be required to integrate with CCTV Surveillance System to receive real-time feeds of the camera installed by them. These video feeds will be saved and utilized in Analytical layer to help administration monitor its assets and do a better urban planning.
3	**Integration of Smart Parking**	• KICCC will be required to integrate with the command center of the Smart Parking solution, which is a PAN City initiative. • KICCC will be required to receive feeds on the status of parking across the city which are managed by the Smart Parking command center (feeds received from all the edge devices of the Parking Solution). • These feeds will provide information of available, non-available parking slots, functional and non - functional parking slots. • KICCC will also be required get video feeds from the parking areas on real-time basis. • Such video feeds will only be saved for 7 days. All the information received will also be required to be mapped on the GIS map. • All the information received from the smart parking will also go into the Analytical layer which will help city in better planning and running of operations.
4	**Integration of Solid Waste Mgmt. Services (Tracking of Solid**	• KICCC will be required to integrate with the control room of Solid Waste Vehicle tracking project (Pan City Initiative) to receive feeds on the location of the solid waste vehicles. • KICCC will also get other information which is received in

Sr. No.	List of Services	Brief of Scope for Integration
	Waste Vehicles)	the control room like fuel utilization of Vehicles. • All the information received will also be required to be mapped on the GIS map. • All the information received from the command center will also go into the Analytical layer which will help city in better planning and running of operations. • KICCC should also be able to trigger the commands / alerts (if required) to the respective command center.
5	**Integration of VMC Call Centre & VMC Services**	• KICCC will be required to integrate its helpdesk and system with VMC call center, in case if there is some information or notification is to be sent to • VMC call center for doing some action in the field regarding Municipal Corporation work. • All the information received from the command center will also go into the Analytical layer which will help city in better planning and running of operations. • KICCC will be required to integrate with the backend system of Varanasi Municipal Corporation. • KICCC should be able to integrate with the existing ICT systems and edge / end / mobile devices of various VMC departments such as Garden, General Administration Department, Water Supply, Sewerage, Assessment and Collection (Property Tax, Shops and establishment), Fire (Fire Brigade Section), Transport of Heavy Vehicles and Maintenance (Workshop), Audit and License Issue to receive and send information. • KICCC should be able to map the data received from various VMC departments on its GIS Platform. • KICCC will be required to send VMC field agents, alerts and notifications for any emergency / incidents / disaster in the city for doing required action. • KICCC system should also be able to get acknowledgement from the receivers.

Sr. No.	List of Services	Brief of Scope for Integration
6	**Integration with Varanasi Smart MAP (GIS)**	• KICCC will be required to use the GIS platform developed by VSCDCL for the city. • There will be a requirement for enhancing the existing platform and using it in the KICCC for doing all the necessary actions. • All the information received from the application will also go into the Analytical layer which will help city in better planning and running of operations.
7	**Integration with Environmental Sensors**	• KICCC will be required to integrate with Environmental Sensors to receive real-time feeds from them. • These feeds will be saved and utilized in Analytical layer to help administration monitor its assets and do a better urban planning.
8	**Integration with Power Grid for making Utilities Dashboard**	• KICCC will be required to integrate with Power Grid network with Varanasi city on GIS Map (If required). • The Smart grid poject related data and reports (as per requirement of VSCL) should be integrated into KICCC Dashboard which should be seamless integration as one component.
9	**Integration with Smart Lights**	• KICCC will be required to integrate with Smart Lights Grid network with Varanasi city on GIS Map. • All functionalities of the LED lights (existing) should be Geo Tagged on Varanasi GIS map that provides full functional and operational features in KICCC dashboard. • The Smart light project should be integrated into KICCC Dashboard which should be seamless integration as one component
10	**Integration with Project 311/ 112**	• Govt. of UP has envisaged 311 scheme which needs to be linked with the proposed system. • The proposed scheme 112 of Govt. of India will also be linked to the proposed system.

Technical Requirements:

Video Wall Screen

Sr. No.	Parameter	Minimum Specifications
1	**Size**	Screen unit size- 70 ” in 7 * 3 array arrangement
2	**Resolution**	Full high definition (1920 x 1080); 16:9 Widescreen
3	**Dynamic Contrast ratio**	1000000:01 or more
4	**Brightness**	Minimum 250 nits and should be adjustable for lower or even higher brightness requirements Uniformity: >=98%
5	**Viewing angle**	178 degree/178 degree (H/V)
6	**Screen to screen gap**	< 1 mm or better
7	**Light Source Type**	• Best in class LED light source with redundancies for LEDs.
8	**Dust Prevention**	Should be designed to avoid dust / Dust tight and resistant / Follow standards as prescribed by Government
9	**Response time**	8ms
10	**Input**	HDMI
11	**Control**	• On Screen Display (OSD) • IR remote control
12	**Operations**	24 x 7 basis
13	**Power Consumption**	Less than 250 watts per cube or more. Hot swappable power supply. This should be built inside the cube for fail safe operation with cooling features.
14	**Colour and Brightness**	All cubes should have uniform brightness and color. The color calibration should be automatic and continuous operations.

Video Wall Controller

S.No.	Parameter	Minimum Specifications
1	**Controller**	Controller to control Video wall in a matrix arrangement as per

S.No.	Parameter	Minimum Specifications
		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 or more
6	**HDD**	500 GB (7200 RPM) or more
7	**Networking**	Dual-port Gigabit Ethernet Controller with RJ-45 ports
8	**RAID**	RAID 0, 1 or better
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
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
21	**Architecture**	The controller should be based on distributed architecture. The controller should be used to decode the IP camera on the video wall

Video Wall Management Software (VMS)

S.No.	Parameter	Minimum Specifications
1	**Display & Scaling**	Display multiple sources anywhere on display up to any size
2	**Input Management**	All input sources can be displayed on the video wall in freely resizable and movable windows

S.No.	Parameter	Minimum Specifications
3	**Scenarios management**	Save and load desktop layouts from local or remote machines
4	**Layout Management**	Support all layout from input sources, Internet Explorer, desktop and remote desktop application
5	**Multi View Option**	Multiple view of portions or regions of Desktop, multiple application can view from single desktop
6	**Other features**	SMTP support
		Remote Control over LAN
		Alarm management
		Remote management
		Multiple concurrent client
		KVM support
7	**Cube Management**	Cube Health Monitoring
		Pop-Up Alert Service
		Graphical User Interface
8	**Remote Viewing**	The video wall content will be able to show live on any remote display .Mobile with IE
9	**Integration**	The video wall software should have tight integration with VMS and KICCC application

Monitoring Workstations

S.No.	Parameter	Minimum Specifications
1	**Processor**	Latest generation 64bit X86 Quad core processor(3Ghz) or better
2	**Chipset**	Latest series 64bit Chipset
3	**Motherboard**	OEM Motherboard
4	**RAM**	Minimum 8 GB DDR3 ECC Memory @ 1600 Mhz. Slots should be free for future upgrade. Minimum 4 DIMM slots, supporting up to 32GB ECC
5	**Graphics card**	Minimum Graphics card with 2 GB video memory (non- shared)
6	**HDD**	2 TB SATA-3 Hard drive @7200 rpm with Flash Cache of 64GB SSD. Provision for installing 4 more drives.
7	**Media Drive**	No CD / DVD Drive
8	**Network interface**	10/100/1000 Mbps autosensing on board integrated RJ-45 Ethernet port.
9	**Audio**	Line/Mic IN, Line-out/Spr Out (3.5 mm)

S.No.	Parameter	Minimum Specifications
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 ICMCC)**	• 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.

IP Phone

Sr. No.	Parameter	Minimum Specifications
1	Display	2 line or more, Monochrome display for viewing features like messages, directory
2	Integral switch	10/100 mbps for a direct connection to a 10/100BASE-T Ethernet network through an RJ-45 interface
3	Speaker Phone	Yes
4	Headset	Wired, Cushion Padded Dual Ear- Speaker, Noise Cancelling headset with mouthpiece microphone, port compatibility with IP Phone
5	VoIP Protocol	SIP V2
6	POE	IEEE 802.3af or better and AC Power Adpater (Option)

7	Supported Protocols	SNMP, DHCP, DNS
8	Codecs	G.711, G.722, G.729 including handset and speakerphone
9	Speaker Phone	Full duplex speaker phone with echo cancellation Speaker on/off button, microphone mute
10	Volume control	Easy decibel level adjustment for speaker phone, handset and ringer
11	Phonebook/Address book	Minimum 100 contacts
12	Call Logs	Access to missed, received, and placed calls. (Minimum 20 overall)
13	Clock	Time and Date on display
14	Ringer	Selectable Ringer tone
15	Directory Access	LDAP standard directory

IP PBX

Sr. No.	Feature Description
1	The IP telephony system should be a converged communication System with ability to run analog and IP on the same platform using same software load based on server and Gateway architecture
2	The single IP PBX system should be scalable to support up to 500 stations (any mix/percentage of Analog/IP) to achieve the future capacity
3	The system should be based on server gateway architecture with external server running on Linux OS. No. of card based processor systems should be quoted.
4	The voice network architecture and call control functionality should be based on SIP
5	The call control system should be fully redundant solution with no single point of failure & should provide 1:1 redundancy.
6	The communication server and gateway should support IP V6 from day one so as to be future proof
7	The entire solution (IP PBX, its hardware, IP Phones, Voice Gateway) should be from a single OEM
Support for call-processing and call-control	
8	Should support signalling standards/Protocols – SIP, MGCP, H.323, Q.Sig
9	Voice Codec support - G.711, G.729, G.729ab, g.722, ILBC
10	The System should have GUI support web based management console

Security	
11	The protection of signaling connections over IP by means of authentication, Integrity and encryption should be carried out using TLS
12	System should support MLPP feature
13	Proposed system should support SRTP for media encryption and signaling encryption by TLS
14	Secure HTTP support for Call Server Administration, Serviceability, User Pages, and Call Detail Record Analysis and Reporting Tool. Should support Secure Sockets Layer (SSL) for directory
15	The administrator logging on to the call control server needs to authenticate by suitable mechanism such as User Login Information and Passwords/ Radius Server
16	Voice gateway to be provided with 1 PRI card scalable to 3 PRI in future for PSTN (PRI) line termination.

Desktops

S.No.	Item	Minimum Specifications
1	**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
2	**Memory**	8 GB DDR3 RAM @ 1600 MHz. One DIMM Slot must be free for future upgrade
3	**Motherboard**	OEM Motherboard
4	**Hard Disk Drive**	Minimum 500 GB SATA III Hard Disk @7200 RPM or higher
5	**Audio**	Line/Mic In, Line-out/Speaker Out (3.5 mm)
6	**Network port**	10/100/1000 Mbps auto-sensing on-board integrated RJ-45 Ethernet Port
7	**Wireless Connectivity**	Wireless LAN - 802.11b/g/n/
8	**USB Ports**	Minimum 4 USB ports (out of that 2 must be in front)
9	**Display Port**	1 Display Port (HDMI/VGA) port
10	**Power supply**	Maximum Rating 250 Watts, 80 plus certified power supply
11	**Keyboard**	104 keys Heavy Duty Mechanical Switch Keyboard (USB Interface) with 50 million keystrokes life per switch. Rupee Symbol to be engraved.
12	**Mouse**	Optical with USB interface (same make as desktop)

S.No.	Item	Minimum Specifications
13	**Monitor**	Minimum 18.5" diagonal LED Monitor with 1366x768 or higher resolution. (Same make as desktop). Must be TCO05 certified
14	**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. All Utilities and driver software, bundled in CD/DVD/Pen-drive media
15	**Certification for Desktop**	Energy Star 5.0 or above / BEE star certified
16	**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.

Laptops

Sr. No.	Item	Minimum Specifications
1	**Processor**	Latest generation Intel Core i5 (2 Ghz) or higher OR AMD (2 Ghz) Processor or higher OR Equivalent 64 bit x86 processor
2	**Display**	Minimum 14" Diagonal TFT Widescreen with minimum 1366 x 768 resolution (16:9 ratio)
3	**Memory**	8 GB DDR3 RAM @ must be free for future upgrade
4	**Hard Disk Drive**	Minimum 500 GB SATA HDD @ 5400 rpm
5	**Ports**	3 USB Ports; 1- Gigabit LAN (RJ 45); 1- HDMI/Display port; 1- VGA; 1-headphone/Microphone
6	**Web Camera**	Built in web cam
7	**Wireless Connectivity**	Wireless LAN - 802.11b/g/n/ Bluetooth 3.0
8	**Audio**	Built-in Speakers
9	**Battery backup**	Minimum 4 lithium ion or lithium polymer battery with a backup of minimum 4 hours
10	**Keyboard and Mouse**	84 Keys Windows Compatible keyboard, Integrated Touch Pad.

Sr. No.	Item	Minimum Specifications
11	**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. All Utilities and driver software, bundled in CD/DVD/Pen-drive media
12	**Certification**	Energy Star 5.0 or above / BEE star certified
13	**Weight**	Laptop with battery (without DVD) should not weigh more than 2 Kg
14	**Accessories**	Laptop carrying Back-pack. It must be from same OEM as laptop
15	**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.

Multi-Function Laser Printer

Sr. No.	Parameter	Minimum Specifications
1	**Technology**	Laser
2	**Monthly duty cycle/RMPV (pages)**	200,000/5K-20K
3	**Print speed – simplex (A4)**	Up to 41 ppm
4	**Scan speed – Black/Color simplex**	Up to 50/30 ipm
5	**Scan speed – Black/Color duplex**	Up to19/14 ipm
6	**Scan-to destinations**	Email, Network folder, USB
7	**Processor (MHz)**	600
8	**Memory (MB)**	1,024
9	**Hard disk drive (HDD)/Capacity (GB)**	Yes/240
10	**Connectivity**	2 Hi-Speed USB 2.0; 1 Gigabit Ethernet 10/100/1000T network
11	**Print resolution – Max/Best print quality (dpi)**	Up to 1200x1200
12	**Input capacity – Std/Max (sheets)**	600/4,600
13	**Output size – Min/ Max (mm)**	76.2 x127/312x469.9

Sr. No.	Parameter	Minimum Specifications
14	**Automatic duplex**	Yes
15	**Energy Efficiency**	BEE or Energy Star certified
16	**Control panel display**	20 m touchscreen

Laser Printer

Sr. No.	Parameter	Minimum Specifications
1	**Print speed black (normal, A4)**	Up to 25 ppm
2	**Print quality black (best)**	Up to 1200 x 1200 dpi
3	**Print technology**	Monochrome Laser
4	**Duty cycle (monthly, A4)**	Up to 15,000 pages
5	**Recommended monthly page**	volume 250 to 2000
6	**Standard memory**	Minimum 128 MB
7	**Processor speed**	Minimum 700 MHz
8	**Paper handling standard/input**	Up to 250-sheet input tray
9	**Paper handling standard/output**	Up to 150-sheet output bin
10	**Media sizes supported**	A4, A5, A6, B5, postcard
11	**Media types supported**	Paper, transparencies, postcards, envelopes, labels
12	**Standard connectivity**	Hi-Speed USB 2.0 port with USB data cable, Ethernet with RJ45 connectivity
13	**Duplex printing**	Automatic (standard)
14	**Compatible operating systems**	Microsoft Windows 7 Professional(64bit), Windows 8 Pro(64 bit), Windows 8.1, Windows 10, Server 2008 R2, Server 2012 R2, MAC OS 9.0, MAC OS X, Linux
15	**Power requirements:**	Input voltage 220 to 240 VAC (+/- 10%), 50 Hz (+/- 2 Hz);
16	**Power consumption during printing**	Less than 500W
17	**Energy Efficiency**	BEE or Energy Star certified
18	**Front operating Panel**	Graphical LCD display

Projector

Sr. No.	Item	Minimum Specifications
1	**Display Technology**	Poly-silicon TFT LCD
2	**Resolution**	HD 1080p
3	**Colors**	16.7 million Colors
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

Online UPS

Sr. No.	Parameter	Minimum Specifications
1	**Capacity**	Adequate capacity to cover all above IT Components at respective location
2	**Output Wave Form**	Pure Sine wave
3	**Input Power Factor at Full Load**	>0.90
4	**Input**	Three Phase 3 Wire for over 5 KVA
5	**Input Voltage Range**	305-475VAC at Full Load
6	**Input Frequency**	50Hz +/- 3 Hz
7	**Output Voltage**	400V AC, Three Phase for over 5 KVA UPS
8	**Output Frequency**	50Hz+/- 0.5% (Free running); +/- 3% (Sync. Mode)
9	**Inverter efficiency**	>90%
10	**Over All AC-AC**	>85%

Sr. No.	Parameter	Minimum Specifications
	Efficiency	
11	**Technology**	• True Online Double Conversion • IGBT technology • PWM inverter switching technology
12	**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
13	**Battery Backup**	60 minutes in full load
14	**Battery**	VRLA (Valve Regulated Lead Acid) SMF (Sealed Maintenance Free) Battery
15	**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.
16	**Audio Alarm**	Battery low, Mains Failure, Over temperature, Inverter overload, Fault etc.
17	**Cabinet**	Rack / Tower type, 75KW/ 150KW/ 200KW configurations
18	**Operating Temp**	0 to 40 degrees centigrade

Diesel Genset

Sr. No.	Item	Minimum Specifications
1	**General Specifications**	a) Auto Starting DG Set mounted on a common base frame with AVM (Anti-Vibration) pads, residential silencer with exhaust piping, complete conforming to ISO 8528 specifications and CPCB certified for emissions. b) KVA rating as per the requirement to provide the supply for KICCC and data center
2	**Engine**	Radiator cooled, multi cylinder, 1500 RPM diesel engine, with electronic/manual governor and electrical starting arrangement complete with battery, conforming to BS 5514/ ISO 3046/ IS 10002
3	**Fuel**	High Speed Diesel (HSD)

Sr. No.	Item	Minimum Specifications
5	**Alternator**	Self-exciting, self-regulating type alternator rated at 0.8 PF or better, 415 Volts, 3 Phase, 4 wires, 50 cycles/sec, 1500 RPM, conforming to IS 4722/ BS 5000, Windings of 100% Copper, class H insulation, Protection as per IP 23.
6	**AMF (Auto Main Failure) Panel**	AMF Panel fitted inside the enclosure, with the following: It should have the following meters/indicators: • Incoming and outgoing voltage • Current in all phases • Frequency • KVA and power factor • Time indication for hours/minutes of operation • Fuel Level in fuel tank, low fuel indication • Emergency Stop button • Auto/Manual/Test selector switch • MCCB/Circuit breaker for short-circuit and overload protection • Control Fuses • Earth Terminal • Any other switch, instrument, relay etc. essential for Automatic functioning of DG set with AMF panel
7	**Acoustic Enclosure**	The DG set shall be provided with acoustic enclosure / canopy to reduce the sound level and to house the entire DG set (Engine & Alternator set) assembly outside (open-air). The enclosure must be weather resistant powder coated, with insulation designed to meet latest MOEF/CPCB norms for DG sets, capable to withstand climate. The enclosure must have ventilation system, doors for easy access for maintenance, secure locking arrangements etc.
8	**Fuel Tank Capacity**	It should be sufficient and suitable for containing fuel for minimum 12 hours continuous operation, Complete with level indicator, fuel inlet and outlet, air vent, drain plug, inlet arrangement for direct filling and set of fuel hoses for inlet and return.

Fixed Dome Camera for Indoor Surveillance

Refer City Surveillance Technical Specifications – Fixed Dome Camera.

4.2 Data Center (DC) & Disaster Recovery (DR)

Data Center

- MSI is required to co-locate all the hardware/software and related items for the smart city infrastructure including SLA monitoring and Help Desk Management, in a Tier III or above data Center complying to standard guidelines as per Telecommunications Infrastructure UPTIME/TIA-942.

- The Data center shall be available for 24x7x365 operation.

- The smart city infrastructure shall have built in redundancy and high availability in compute and storage to ensure that there is no single point of failure.

- The MSI is free to take the colocation services from any existing data center located within India (preferably in the same city where possible) which meets the prevailing data center standards, since this is one of the most critical components of the smart city infrastructure. However, the system SLA as defined in the tender to be met solely by the MSI.

- The MSI shall submit to Authority adequate documentation/ evidences in support of the choice of the data center to meet the project requirements.

- Min Guiding factors for selection of the Data Center**:** Following are the benchmark requirements which should act as guiding factors for the MSI to select and propose the locations for the Data Center

- There should be dedicated rack space available in the data center for the entire Smart City Project Infrastructure.

- Access to the Data Center Space where the Smart City Project Infrastructure is proposed to be hosted should be demarcated and physical access to the place would be given only to the authorized personnel

- Racks to be caged.

- Smart City Data Center should be at least a Tier III Data Center as per Telecommunications Infrastructure Standard for Data Centers and should be 27001 Certified. The required certification to be enclosed along with the technical bid response.

- It should have access control system implemented for secured access.

- Indoor CCTV Cameras would be required to be installed to monitor the physical access of the system from remote location

- Physical Access to the building hosting Data Center should be armed and it must be possible to even depute police personnel for physical security of the premises.

- Min 90 days Data Backup of the video feeds and the transaction data for min 1 year shall be stored within the Data Center Infrastructure preferable in a cost effective and innovative manner.

- In case the data center services are to go down due to any unforeseen circumstance, the Command Center should have access to the video feeds of previous 90 days and the transaction data for min 1 year from this data backup facility.

- Access logs to be stored for the entire duration of contract and handed over to Authority upon termination/expiry of the contract.

- MSI should optimize the overall system within intranet and internet communications during maintenance phases based on utilization of applications and submit reports accordingly

- Enterprise Management System and Network and Security Management Solution.

- Centralized System for Security Solution.

Functional Specifications- DC/ DR:

Data Center specifications:

- Design Standard: Tier-III or above

- The availability of data must be guaranteeing to 99.982% availability.

- Receiving Power: Commercial power substation next to DC
- UPS: UPS system with N+N redundancy
- Generator: Gen-set with N+1 redundancy
- Power Provision: Dual power feed, PDU sources to each rack, Power supply to a rack as per requirement

Databases

Any commercially available database (with OEM Warranty) shall be provided along with license and support & upgrade costs.

Sr. No.	Parameters
	General
1	Database License should be un-restricted, to prevent any non-compliance in an event of customization & integration.
2	Database should provide Unicode (Latest version) capability with Indian language support
3	Databases shall support multi hardware and Operating System platform.
4	Database shall provide standard access Tool for administering the database. The tool should be able to monitor, maintain and manage the database instance, objects, and packages.
5	Database shall have built-in backup and recovery tool, which can support the online backup.
6	Database shall be able to provide database level storage management mechanism, which should enable the availability by means of creating redundancy, automatically balance the data files across the available disks, i/o balancing across the available disks for the database for performance, availability and management.

Sr. No.	Parameters
8	Should be an enterprise class database with the ability to support connection pooling, load sharing and load balancing when the load on the application increases.
9	Database shall provide native functionality to store XML, within the database and support search, query functionalities.
10	Database shall have built-in DR solution to replicate the changes happening in the database across DR site with an option to run real-time reports from the DR site without stopping the recovery mechanism.
11	Database shall have Active-Passive failover clustering with objectives of scalability and high availability.
12	Database shall provide mechanism to recover rows, tables when accidentally deleted. The mechanism should provide ways and means of recovering the database.
13	Database shall provide functionality to replicate / propagate the data across different databases.
15	The RDBMS should support partitioning feature in table level object.
16	Database shall provide native functionality to store XML, Images, Text, Medical Images, CAD images within the database and support search, query functionalities.
17	Database shall include tools for enterprise class high availability solution like monitoring performance, diagnose and alert for problems, tuning bottlenecks, resource monitoring and automatic resource allocation capabilities.
18	RDBMS must support the SQL queries.
19	Database shall provide security mechanism at foundation level of the database, so that the options and additions to the database confirm the security policy of the organization without changing the application code. Shall confirm to security evaluations and conformance to common criteria.
20	Database shall provide control data access down to the row-level so that multiple users with varying access privileges can share the data within the same physical database.
21	Database shall support for enhanced authentication by integrating tokens and biometric technologies.

Sr. No.	Parameters
22	Database shall provide functionality for classifying data and mediating access to data based on its classification for multi-level security and mandatory access control, manage access to data on a "need to know" basis.
23	Database shall be having native auditing capabilities for the database. Should support optional Audit Capability to store the audit records in separate audit store with monitoring & reporting for multiple databases to detect any security breaches.
24	Database shall be having built-in provision to Administer database / database clusters, Monitor performance, Maintain database, Backup and recovery, Recovery management, Disaster recovery management.
25	The Management tool should provide advisory-based performance tuning tool which help to tune the queries or objects, SQL analysis, SQL access.
26	The enterprise database should provide single web-based console for management of the database.
Restart and Recovery	
27	Availability of recovery/restart facilities of the DBMS.
28	Automated recovery/restart features provided that do not require programmer involvement or system reruns.
29	Program restart should be provided from the point of failure.
30	Ability to manage recovery/restart facilities to reduce system overhead.
31	Provides extra utilities to back up the databases by faster means than record by record retrieval.
32	Provides clear error reporting, recovery and logging.
33	Describe recovery strategies that needs to be in place.

Sr. No.	Parameters
34	System should support mirroring for DRP.
Backup Procedures	
35	Describe Backup Procedures you plan to deploy.
36	Describe backup application(s) your proposed solution use.
37	Provide details of data backup and restore processes and procedures for all data elements.
38	Provide details of automated archiving procedures to copy active data to storage media when archive 'age' is reached.
Error Handling	
39	Ability to trap a transaction failure through: • Application Software • DBMS • Availability of manual containing all system error messages and correction procedures
System Control	
40	Provide details of the 'Audit trail' facility for your proposed solution.
41	Should provide adequate auditing trail facility.
42	System should record the date and time stamp for all records.
43	Ability to track terminals from where the system is accessed.

Networking:

Switching Fabric Architecture

S. No.	Parameter	Specifications

1	**Fabric Definition**	• Fabric is the Clos Architecture defined using Spine, Leaf and VXLAN + ISIS or VXLAN + EVPN Protocol.
		• Fabric should have following functionalities to be achieved:
		  • Flexibility: allows workload mobility anywhere in the DC.
		  • Robustness: while dynamic mobility is allowed on any authorized location of the DC, the failure domain is contained to its smallest zone.
		  • Performance: full cross sectional bandwidth (any-to-any) – all possible equal paths between two endpoints are active.
		  • Deterministic Latency: fix and predictable latency between two endpoints with same hop count between any two endpoints, independently of scale.
		  • Scalability: add as many Leaf as needed to achieve desired scale in terms of number of servers while maintaining the same oversubscription ratio everywhere inside the fabric.

2	**Optics**	Fabric should have Switch and Optics from same OEM.
3	**Fabric Features**	• Fabric must support various Hypervisor encapsulation including VXLAN, NVGRE and 802.1q natively without any additional hardware/software or design change. • Fabric must auto discover all the hardware and auto provision the fabric based on the policy. • The fabric architecture must be based on hardware VXLAN overlays to provide logical topologies that are abstracted from the physical infrastructure with no performance degradation. Fabric must support VXLAN Switching/Bridging and VXLAN Routing. • Fabric must provide open programmable interface using phython SDK, Jason SDK, XMLS or COBRA etc. from the Central Management appliance / SDN Controller for programming/configuring the entire fabric.

		• Fabric must provide open scripting interface using Bash, powershell, NetConf, YANG from the central management appliance / SDN Controller for configuring the entire fabric. • Fabric must support Role Based Access Control in order to support Multi - Tenant environment. • Fabric must integrate with different virtual machine manager and manage virtualise networking from the single pane of Glass - Fabric Controller/SDN Controller. • Fabric must integrate with best of breed L4 - L7 Physical and virtual appliances and manage using single pane of glass - Fabric Controller / SDN Controller. • Fabric must provide deeper visibility into the fabric in terms of latency and packet drop between VM to VM, VM to Physical server and vise versa, Leaf to another leaf etc. • Fabric must act as single distributed layer 2 switch, Layer 3 router and Stateless distributed firewall etc. • Fabric must provide REST APIs from the Central management appliance/SDN Controller in order to integrate with best of breed Management, Monitoring, Hypervisor and Cloud automation & Orchestration software.
4	**Fabric Layer 2, Layer 3 and Misc. Features**	• Fabric must support Layer 2 features like LACP, STP /RSTP /MSTP, VLAN Trunking, LLDP etc. • Fabric must support multi chassis ether channel/MLAG i.e. Host connects to two different Leaf switches and form ether channel using LACP/NIC Teaming on Host. • Fabric must support Jumo Frame upto 9K Bytes on 1G/10G/25G/40G/100G ports. • Fabric must support Layer 2 Multicast i.e. IGMP v1, v2 and v3. • Fabric must support IP v4 and IP v6 FHRP using HSRP or VRRP. • Fabric must support IP v4 and IP v6 Layer 3 routing

		protocol OSPF and BGP. • Fabric must support IP v6 dual stack. • Fabric must support traffic redistribution between different routing protocols. • Fabric must support IP v4 and IP v6 management tools like - Ping, Traceroute, VTY, SSH, TFTP and DNS Lookup. • Fabric must support IP v4 and IP v6 SNMP V1 / V2 / V3. • Fabric must support RMON/RMON-II for monitoring. • Fabric must support integration with the centralised Syslog server for monitoring and audit trail. • Fabric must support NTP.
5	**Fabric Security Features**	• Fabric must have zero trust policy model for connected systems or hosts to help in protecting against any kind of attacks like Unauthorized Access, Man - in - the - middle - attack, Replay Attack, Data Disclosure, Denial of Service. • Fabric must provide RBAC policies and support AAA using Local User authentication, External RADIUS, External TACACS+, External LDAP, External AD. • Fabric must support VM attribute based zoning and policy. • Fabric must support Micro Segmentation for the Virtualize and Non - Virtualize environment. • Fabric must support true multi - tanency . • Fabric must be accessible using CLI over SSH and GUI using HTTP/HTTPS • Fabric must support SNMP v2/3 with HMAC-MD5 or HMAC-SHA authentication and DES encryption. • Fabric must act as a State-less distributed firewall with the logging capability.
6	**Fabric Service Features**	• Fabric must be capable to provide services of L 4 - L7 services using physical or virtual appliances i.e. Firewall, ADC, IPS etc. • Fabric must have zero trust policy model for connected systems or hosts to help in protecting against any kind of attacks like Unauthorized Access, Man - in - the - middle -

		attack, Replay Attack, Data Disclosure, Denial of Service.
7	**Fabric Scale and Performance**	• Fabric should support scale up and scale out without any service disruption. • Fabric must support for 500 VRF/Private network without any additional component or upgrade or design change. • Fabric must scale from 100 Tenant to 500 Tenant without any additional component or upgrade or design change. • Fabric must integrate with minimum 3 Virtual Machine Manager (i.e. vCenter, SCVMM, OpenStack etc.) of different Hypervisors simultaneously and scalable to 5 in future with or without common orchestrator. • Fabric must be capable of connecting 2500 physical servers and scale to 5000 physical servers.. • Fabric must be capable of integrating minimum of 8 nos. of L 4 - L7 services physical or virtual appliances (i.e. Firewall, ADC, IPS etc.) and scale upto 16 nos of L4 - L7 Services appliances. • Fabric must support minimum of 4 Leaf switches and scale upto 250 Leaf switches without any design change. • Fabric must support minimum of 2 Spine Switches and scale upto 6 Spine switches without any design change. • Spine Switches must have adequate number of line rate 40/100G ports to support desired Leaf Scale. • Each Leaf connects to Each Spine using minimum 1 x 40/100 G ports connectivity i.e. Each Spine must have 128 nos. of line rate 40G/100G ports with consideration of leaf to SPINE over subscription ration of 4:1. • Fabric must support 20K IPv4 and 10K IPv6 routes scalable to 30K IPv4 and 15K IPv6 routes. • Fabric must support 4K multicast groups scalable to 8K multicast groups. • Fabric must support 256 nos. of MLAG/VPC scalable to 384 nos. Each MLAG/VPC must support maximum 8

		member links. • Fabric must support 256 nos. of Port Channel scalable to 384 nos. Each Port Channel must support maximum of 8 member links.
8	**Fabric management**	• Fabric must provide Centralised Management Appliance or SDN Controller - Single pane of Glass for managing, monitoring and provisioning the entire Fabric. • Fabric must Auto discover all the Spine and Leaf switches and auto provision them based on the Fabric policy using Centralised Management appliance or SDN Controller. • Centralised management appliance or SDN Controller must manages and provision L4 - L7 Services physical or virtual appliance as well as integrate with Virtual Machine manager. • Centralised management appliance or SDN Controller should not participate in Data plane and control plane path of the fabric. • Centralised management appliance or SDN Controller must provide necessary report for compliance and audit. • Centralised management appliance or SDN Controller must communicate to south bound devices using open standard protocol i.e. OPFLEX, OPENFLOW, OVSDB etc. or using Device APIs. • Centralised management appliance or SDN Controller communication with the south bound devices must be encrypted • Centralised management appliance or SDN Controller must communicate with the south bound devices using more than one path i.e. in-path connectivity and out of band management connectivity • Centralised management appliance or SDN Controller provide dynamic device inventory of the Fabric as well as current network topology of the fabric. It must also validate the cabling connectivity and generate alarms in case of wrong or faulty connectivity. • Centralised management appliance or SDN Controller must

		run in "N + 1 or N + 2" redundancy to provide availability as well as function during the split brain scenario.

Spine Switch Specifications:

Sr. No.	Parameter	Specifications
1	**Solution Requirement**	Minimum 2 number of Spine switches should be provided. If the solution requires more number of spine switches, the same shall be provided by the bidder.
2	**General Requirement**	The core/spine layer switches should have hardware level redundancy (1+1) in terms of data plane and control plane. Issues with any of the plane should not impact the functioning of the switch. All the switches should be from same OEM.
		The switch should have redundant CPUs working in active-active or active-standby mode. CPU fail over/change over should not disrupt/impact/degrade the functioning the switch.
		The Switch should support non-blocking Layer 2 switching and Layer 3 routing
		The switch should not have any single point of failure like CPU, supervisor, switching fabric power supplies and fans etc should have 1:1/N+1 level of redundancy
		Switch should support in line hot insertion and removal of different parts like modules/power supplies/fan tray etc. This should not require rebooting of the switch or create disruption in the working/functionality of the switch
		Switch should support the complete STACK of IP V4 and IP V6 services. Switch must have IPv6 phase 2 ready logo certification.
		Switch with different modules should function line rate and should not have any port with oversubscription ratio applied
		Switch should support in service software upgrade of the switch without disturbing the traffic flow. There should not be any impact on the performance in the event of the software upgrade/downgrade. It should support in service patching of

		selected process/processes only without impacting other running processes
		Switch should support non-blocking, wire speed performance per line card
3	**Hardware and Interface Requirement**	Switch should have the following interfaces: 36 nos. of line rate and Non - Blocking 40/100G ports
		Switch should have min 80MB buffer
		Switch should have EAL2/NDPP certified
		Switch should have console port for local management
		Switch should have management interface for Out of Band Management
		Switch should be rack mountable and support side rails, if required
		Switch should have adequate power supplies for the complete system usage with all slots populated and used, providing N+1 redundancy
		Switch should have hardware health monitoring capabilities and should provide different parameters through SNMP
		Switch should support VLAN tagging (IEEE 802.1q)
		Switch should support IEEE Link Aggregation and Ethernet Bonding functionality to group multiple ports for redundancy
		Switch should have the capability of holding multiple OS images to support resilience & easy rollbacks during the version upgrades etc and should support in service software upgrade including: • Multiple System image • Multiple system configuration • Option of Configuration roll-back
		Switch should support for different logical interface types like loopback, VLAN, SVI, Port Channel, multi chassis port channel/Link Aggregation Group (LAG) etc
4	**Performance Requirement**	The switch should support 1,20,000 IPv4 and IPv6 routes entries in the routing table with multicast routes
		Switch should support Graceful Restart for OSPF, BGP etc.
		Switch should support minimum 1000 VRF instances
		The switch should support uninterrupted forwarding operation for

		OSPF, BGP etc. routing protocol to ensure high-availability during primary controller failure
		The switch should support hardware based load-balancing at wire speed using LACP and multi chassis etherchannel/LAG
		Switch should support total aggregate minimum 32 Tbps minimum of switching capacity including the services: • Switching • IP Routing (Static/Dynamic) • IP Forwarding • Policy Based Routing • QoS • ACL and Other IP Services • IP V.6 host and IP V.6 routing
5	**Virtualization Features**	Switch should support Network Virtualisation using Virtual Over Lay Network using VXLAN (RFC 7348)/NVGRE as per RFC 2890
		Switch should support VXLAN (RFC7348) and EVPN or equivalent for supporting Spine - Leaf architecture to optimise the east - west traffic flow inside the data center
		Switch should support Open Flow/Open Day light/Open Stack controller
		Switch should support Data Center Bridging
		Switch should support multi OEM hypervisor environment and should be able to sense movement of VM and configure network automatically
6	**Layer2 Features**	Spanning Tree Protocol (IEEE 802.1D, 802.1W, 802.1S
		Switch should support VLAN Trunking (802.1q) and should support 4096 VLAN
		Switch should support basic Multicast IGMP v1, v2, v3
		Switch should support minimum 160,000 no. of MAC addresses
		Switch should support 16 Nos. of link or more per Port channel (using LACP) and support 200 port channels or more per switch
		Switch should support Industry Standard Port/Link Aggregation for All Ports across any module or any port.
		Switch should support multi chassis Link Aggregation for All Ports

		across any module or any port of the switch and Link aggregation should support 802.3ad LACP protocol for communication with downlink/uplink any third party switch or server. Spine to spine - minimum 16 port Multi Chasis etherchannel/LAG should be provided.
		Switch should support Jumbo Frames up to 9K Bytes on 1G/10G Ports
		Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities
		Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures
7	**Layer3 Features**	Switch should support all physical ports to use either in Layer2 or Layer 3 mode and also should support layer 3 VLAN Interface and Loopback port Interface
		Switch should support basic routing feature i.e. IP Classless, default routing and Inter VLAN routing
		Switch should support static and dynamic routing using: • Static routing • OSPF V.2 using MD5 Authentication • ISIS using MD5 Authentication • BGP V.4 using MD5 Authentication • Should support route redistribution between these protocols • Should be compliant to RFC 4760 Multiprotocol • Extensions for BGP-4 (Desirable)
		Switch should reconverge all dynamic routing protocol at the time of routing update changes i.e. Non-Stop forwarding for fast re-convergence of routing protocols
		Switch should support multi instance MPLS routing using VRF, VRF Edge routing and should support VRF Route leaking functionality
		Switch should be capable to work as DHCP server and relay

		Switch should provide multicast traffic reachable using: • PIM-SM • PIM-SSM • Bi-Directional PIM • Support RFC 3618 Multicast Source Discovery Protocol (MSDP) • IGMP V.1, V.2 and V.3
		Switch should support Multicast routing ECMP
8	**Availability**	Switch should have provisioning for connecting to 1:1/N+1 power supply for usage and redundancy
		Switch should provide gateway level of redundancy in Ip V.4 and IP V.6 using HSRP/VRRP
		Switch should support for BFD For Fast Failure Detection as per RFC 5880 and RFC-7419, 3618, 7296, 7427, 7296.
9	**Quality of Service**	Switch system should support 802.1P classification and marking of packet using: • CoS (Class of Service) • DSCP (Differentiated Services Code Point) • Source physical interfaces • Source/destination IP subnet • Protocol types (IP/TCP/UDP) • Source/destination TCP/UDP ports
		Switch should support methods for identifying different types of traffic for better management and resilience
		Switch should support for different type of QoS features for ream time traffic differential treatment using: • Weighted Random Early Detection • Strict Priority Queuing
		Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy
		Switch should support Flow control of Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end for receiving traffic as per IEEE 802.3x

10	**Security**	Switch should support for deploying different security for each logical and physical interface using Port Based access control lists of Layer-2 to Layer-4 in IP V.4 and IP V.6 and logging for fault finding and audit trail
		Switch should support control plane i.e. processor and memory Protection from unnecessary or DoS traffic by control plane protection policy
		Time based ACL
		Switch should support for external database for AAA using: • TACACS+ • RADIUS
		Switch should support MAC Address Notification on host join into the network for Audit trails and logging
		Switch should support to restrict end hosts in the network. Secures the access to an access or trunk port based on MAC address. It limits the number of learned MAC addresses to deny MAC address flooding
		Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined
		Switch should support to prevent edge devices in the network not administrator's controlled from becoming Spanning Tree Protocol root nodes
		Switch should support unicast and/or multicast blocking on a switch port to suppress the flooding of frames destined for an unknown unicast or multicast MAC address out of that port
		Switch should support Spanning tree BPDU protection
		Switch should support for MOTD banner displayed on all connected terminals at login and security discrimination messages can be flashed
11	**Manageability**	Switch should support for embedded RMON/RMON-II for central NMS management and monitoring
		Switch should support for sending logs to multiple centralised syslog server for monitoring and audit trail
		Switch should provide remote login for administration using: • Telnet

		• SSH V.2
		Switch should support for capturing packets for identifying application performance using local and remote port mirroring for packet captures
		Switch should support for management and monitoring status using different type of Industry standard NMS using: • SNMP V1 and V.2 • SNMP V.3 with encryption • Filtration of SNMP using Access list • SNMP MIB support for QoS
		Switch should support for basic administrative tools like: • Ping • Traceroute
		Switch should support central time server synchronisation using Network Time Protocol NTP V.4
		Switch should support for providing granular MIB support for different statistics of the physical and logical interfaces
		Switch should support for predefined and customized execution of script for device mange for automatic and scheduled system status update for monitoring and management
		Switch should provide different privilege for login in to the system for monitoring and management
		Switch should support Real time Packet Capture using Wireshark in real time for traffic analysis and fault finding
12	**IPv6 features**	Switch should support for IP V.6 connectivity and routing required for network reachability using different routing protocols such as: • OSPF V.3 • BGP with IP V.6 • IP V.6 Policy based routing • IP V.6 Dual Stack etc • IP V.6 Static Route • IP V.6 Default route • Should support route redistribution between these protocols

		Switch should support multicast routing in IP V.6 network using PIMv2 Sparse Mode
		Switch should support for QoS in IP V.6 network connectivity
		Switch should support for monitoring and management using different versions of SNMP in IP V.6 environment such as: • SNMPv1, SNMPv2c, SNMPv3 • SNMP over IP V.6 with encryption support for SNMP Version 3
		Switch should support syslog for sending system log messages to centralised log server in IP V.6 environment
		Switch should support NTP to provide an accurate and consistent timestamp over IPv6 to synchronize log collection and events

Leaf (Fiber) Switch Specifications:

Sr. No.	Parameter	Specifications
1	**Solution Requirement**	Minimum 4 number of switches should be provided. If the solution requires more number of spine switches, the same shall be provided by the bidder as per requirement.
2	**General Requirement**	The Switch should support non-blocking Layer 2 switching and Layer 3 routing.
		There switch should not have any single point of failure like power supplies and fans etc should have 1:1/N+1 level of redundancy
		Switch support in-line hot insertion and removal of different parts like modules/power supplies/fan tray etc should not require switch reboot and disrupt the functionality of the system
		Switch should support the complete STACK of IP V4 and IP V6 services. Switch must have IPv6 phase 2 ready logo certification.

Sr. No.	Parameter	Specifications
		The Switch and different modules used should function in line rate and should not have any port with oversubscription ratio applied.
3	**Hardware and Interface Requirement**	Switch should have the following interfaces:
		a. 48 x 1G/10G/25G Multi Mode Fiber Interface
		b. 6 x 40/100GbE QSFP ports
		Switch should support native 25gig port(IEEE 802.3BY)
		Switch should have minimum 30MB buffer
		Switch should be EAL2/NDPP Certified
		Switch should have console port
		Switch should have management interface for Out of Band Management
		Switch should be rack mountable and support side rails if required
		Switch should have hardware health monitoring capabilities and should provide different parameters through SNMP
		Switch should support VLAN tagging (IEEE 802.1q)
		Switch should support IEEE Link Aggregation and Ethernet Bonding functionality to group multiple ports for redundancy
		Switch should support Configuration roll-back and check point
		Switch should support for different logical interface types like loopback, VLAN, SVI, Port Channel, multi chassis port channel/LAG etc
4	**Performance Requirement**	The switch should support 1,20,000 IPv4 and IPv6 routes entries in the routing table with multicast routes
		Switch should support Graceful Restart for OSPF, BGP etc.

Sr. No.	Parameter	Specifications
		Switch should support minimum 1000 VRF instances
		The switch should support uninterrupted forwarding operation for OSPF, BGP etc. routing protocol to ensure high-availability during primary controller failure
		The switch should support hardware based loadbalancing at wire speed using LACP and multi chassis etherchannel/LAG
		Switch should support total aggregate minimum 32 Tbps minimum of switching capacity including the services: a. Switching b. IP Routing (Static/Dynamic) c. IP Forwarding d. Policy Based Routing e. QoS f. ACL and Other IP Services g. IP V.6 host and IP V.6 routing
		Each leaf should have connectivity to all spine switches and the over subscription should not be less then 4:1
5	**Advance Features**	Switch should support Network Virtualisation using Virtual Over Lay Network using VXLAN (RFC 7348)/NVGRE as per RFC 2890
		Switch should support VXLAN (RFC7348) and EVPN or equivalent for supporting Spine - Leaf architecture to optimise the east - west traffic flow inside the data center
		Switch should support Open Flow/Open Day light/Open Stack controller
		Switch should support Data Center Bridging
		Switch should support multi OEM hypervisor environment and should be able to sense movement of VM and configure network automatically
6	**Layer2 Features**	Spanning Tree Protocol (IEEE 802.1D, 802.1W, 802.1S
		Switch should support VLAN Trunking (802.1q) and should

Sr. No.	Parameter	Specifications
		support 4096 VLAN
		Switch should support basic Multicast IGMP v1, v2, v3
		Switch should support minimum 160,000 no. of MAC addresses
		Switch should support 16 Nos. of link or more per Port channel (using LACP) and support 200 port channels or more per switch
		Switch should support Industry Standard Port/Link Aggregation for All Ports across any module or any port.
		Switch should support multi chassis Link Aggregation for All Ports across any module or any port of the switch and Link aggregation should support 802.3ad LACP protocol for communication with downlink/uplink any third party switch or server. Spine to spine - minimum 16 port Multi Chasis etherchannel/LAG should be provided.
		Switch should support Jumbo Frames up to 9K Bytes on 1G/10G Ports
		Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities
		Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures
7	**Layer3 Features**	Switch should support all physical ports to use either in Layer2 or Layer 3 mode and also should support layer 3 VLAN Interface and Loopback port Interface
		Switch should support basic routing feature i.e. IP Classless, default routing and Inter VLAN routing

Sr. No.	Parameter	Specifications
		Switch should support static and dynamic routing using: a. Static routing b. OSPF V.2 using MD5 Authentication c. ISIS using MD5 Authentication d. BGP V.4 using MD5 Authentication e. Should support route redistribution between these protocols f. Should be compliant to RFC 4760 Multiprotocol Extensions for BGP-4 (Desirable)
		Switch should re-converge all dynamic routing protocol at the time of routing update changes i.e. Non-Stop forwarding for fast re-convergence of routing protocols
		Switch should support multi instance MPLS routing using VRF, VRF Edge routing and should support VRF Route leaking functionality
		Switch should be capable to work as DHCP server and relay
		Switch should provide multicast traffic reachable using: a. PIM-SM b. PIM-SSM c. Bi-Directional PIM d. Support RFC 3618 Multicast Source Discovery Protocol (MSDP) e. IGMP V.1, V.2 and V.3
		Switch should support Multicast routing ECMP
8	**Availability**	Switch should have provisioning for connecting to 1:1/N+1 power supply for usage and redundancy
		Switch should provide gateway level of redundancy in Ip V.4 and IP V.6 using HSRP/VRRP
		Switch should support for BFD For Fast Failure Detection as per RFC 5880 and RFC-7419, 3618, 7296, 7427, 7296.

Sr. No.	Parameter	Specifications
9	**Quality of Service**	Switch system should support 802.1P classification and marking of packet using: a. CoS (Class of Service) b. DSCP (Differentiated Services Code Point) c. Source physical interfaces d. Source/destination IP subnet e. Protocol types (IP/TCP/UDP) f. Source/destination TCP/UDP ports
		Switch should support methods for identifying different types of traffic for better management and resilience
		Switch should support for different type of QoS features for ream time traffic differential treatment using a. Weighted Random Early Detection b. Strict Priority Queuing
		Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy
		Switch should support Flow control of Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end for receiving traffic as per IEEE 802.3x
10	**Security**	Switch should support for deploying different security for each logical and physical interface using Port Based access control lists of Layer-2 to Layer-4 in IP V.4 and IP V.6 and logging for fault finding and audit trail
		Switch should support control plane i.e. processor and memory Protection from unnecessary or DoS traffic by control plane protection policy
		Time based ACL
		Switch should support for external database for AAA using: a. TACACS+ b. RADIUS

Sr. No.	Parameter	Specifications
		Switch should support MAC Address Notification on host join into the network for Audit trails and logging
		Switch should support to restrict end hosts in the network. Secures the access to an access or trunk port based on MAC address. It limits the number of learned MAC addresses to deny MAC address flooding
		Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined
		Switch should support to prevent edge devices in the network not administrator's controlled from becoming Spanning Tree Protocol root nodes
		Switch should support unicast and/or multicast blocking on a switch port to suppress the flooding of frames destined for an unknown unicast or multicast MAC address out of that port
		Switch should support Spanning tree BPDU protection
		Switch should support for MOTD banner displayed on all connected terminals at login and security discrimination messages can be flashed as per banks ISD rules
11	**Manageability**	Switch should support for embedded RMON/RMON-II for central NMS management and monitoring
		Switch should support for sending logs to multiple centralised syslog server for monitoring and audit trail
		Switch should provide remote login for administration using: a. Telnet b. SSH V.2
		Switch should support for capturing packets for identifying application performance using local and remote port mirroring for packet captures

Sr. No.	Parameter	Specifications
		Switch should support for management and monitoring status using different type of Industry standard NMS using: a. SNMP V1 and V.2 b. SNMP V.3 with encryption c. Filtration of SNMP using Access list d. SNMP MIB support for QoS
		Switch should support for basic administrative tools like: a. Ping b. Traceroute
		Switch should support central time server synchronisation using Network Time Protocol NTP V.4
		Switch should support for providing granular MIB support for different statistics of the physical and logical interfaces
		Switch should support for predefined and customized execution of script for device mange for automatic and scheduled system status update for monitoring and management
		Switch should provide different privilege for login in to the system for monitoring and management
		Switch should support Real time Packet Capture using Wireshark in real time for traffic analysis and fault finding
	IPv6 features	Switch should support for IP V.6 connectivity and routing required for network reachability using different routing protocols such as: a. OSPF V.3 b. BGP with IP V.6 c. IP V.6 Policy based routing d. IP V.6 Dual Stack etc e. IP V.6 Static Route f. IP V.6 Default route g. Should support route redistribution between these protocols
		Switch should support multicast routing in IP V.6 network using PIMv2 Sparse Mode

Sr. No.	Parameter	Specifications
		Switch should support for QoS in IP V.6 network connectivity
		Switch should support for monitoring and management using different versions of SNMP in IP V.6 environment such as: a. SNMPv1, SNMPv2c, SNMPv3 b. SNMP over IP V.6 with encryption support for SNMP Version 3
		Switch should support syslog for sending system log messages to centralised log server in IP V.6 environment
		Switch should support NTP to provide an accurate and consistent timestamp over IPv6 to synchronize log collection and events
		Switch should support for IP V.6 different types of tools for administration and management such as:
		a. Ping b. Trace route c. VTY d. SSH e. DNS lookup

Core/SAN Fiber Switch Specifications:

Sr. No.	Parameter
1	The fibre channel switch must be rack-mountable. Thereafter, all reference to the 'switch' shall pertain to the 'fibre channel switch'
2	The switch to be configured with minimum of 96 ports 16 Gbps FC configuration backward compatible to 4/8.
3	All 96 x FC ports for device connectivity should be 4/8/16 Gbps auto-sensing Fibre Channel ports.
4	The switch must have hot-swappable redundant power supply & fan module without resetting the switch, or affecting the operations of the switch.
5	The switch must be able to support non-disruptive software upgrade.
6	The switch must be able to support stateful process restart.

7	The switch must be capable of creating multiple hardware-based isolated Virtual Fabric (ANSI T11) instances. Each Virtual Fabric instance within the switch should be capable of being zoned like a typical SAN and maintains its own fabric services, zoning database, Name Servers and FSPF processes etc. for added scalability and resilience.
8	The switch must support up to 32 Virtual Fabric Instances.
9	The switch must be capable of supporting hardware-based routing between Virtual Fabric instances.
10	The switch must support graceful process restart and shutdown of a Virtual Fabric instance without impacting the operations of other Virtual Fabric instances.
11	The switch shall support hot-swappable Small Form Factor Pluggable (SFP) LC typed transceivers.
12	The switch must support hardware ACL-based Port Security, Virtual SANs (VSANs), and Port Zoning.
13	The switch must support Smart Zoning such that the entries in the TCAM is significantly reduced and therefore increasing the overall scalability of the SAN Fabric.
14	The switch must support PowerOn Auto Provisioning (POAP) and Quick Configuration Wizard for simplified operations.
15	Inter-switch links must support the transport of multiple Virtual Fabrics between switches, whilst preserving the security between Virtual Fabrics.
16	The switch must support routing between Virtual Fabric instance in hardware.
17	The switch shall support FC-SP for host-to-switch and switch-to-switch authentication.
18	The switch must be able to load balance traffic through an aggregated link with Source ID and Destination ID. The support for load balancing utilizing the Exchange ID must also be supported.
19	The switch must be equipped with congestion control mechanisms such that it is able to throttle back traffic away from a congested link.
20	The switch must be capable of discovering neighboring switches and identify the neighboring Fibre Channel or Ethernet switches.
21	The switch should support IPv6. It should support native switch based RESTful APIs
22	The bidder must provide atleast 2 of these switches
23	The interface requirment mentioned here is the minimum. If the solution requires more number of interfaces (considering 100% redundancy) then the same should be qouted

	by the bidder

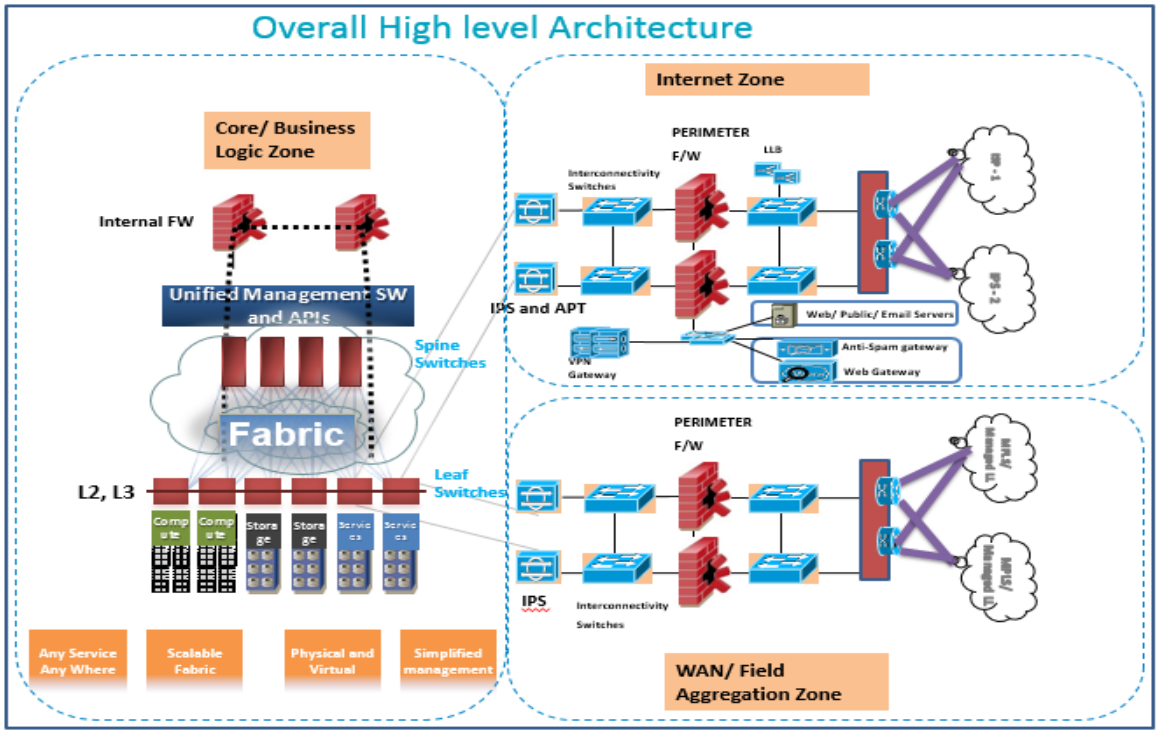


Figure: Illustrative High Level Network Architecture Diagram

Hyper-Converged Infrastructure:

Sr. No.	Parameter
1	The Proposed Solution should be in leaders quadrant for Integrated systems from consecutive last two years.
2	The proposed HCI solution should be 100% software defined and should not use any hardware based RAID, Compression or De-duplication
3	The proposed solution HCI should run on industry standard x86 servers.
4	The proposed solution independently scale storage and compute as and when needed without any downtime. HCI should support storage expansion and compute expansion to extend storage/compute capacity as and when needed.
5	The proposed HCI solution must have metadata distributed on all nodes in a cluster i.e. each node in the cluster should carry information about data lying across every node in

	the cluster
6	The proposed solution must have capability to support nodes with same/different CPU & Memory configurations in the same cluster
7	The proposed solution must have capability to support SSD & SAS/SATA
8	Thin provisioning of both storage entities and virtual machine hard disks
9	The solution should provide automatic failover for hardware failure
10	The solution should support industry protocols NFS/SMB/iSCSI
11	Shall support automated chassis redundancy and survive the failure of entire chassis containing multiple nodes. In a multi-chassis configuration the infrastructure must intelligently distribute data across chassis so no redundant copies of data exist on the same chassis or node.
12	Shall support minimum 32 nodes in a same cluster.
13	The solution support for automated upgrades of storage controllers through management GUI with no downtime and major impact on production
14	Support for layer-2 VLAN for networking and integrated VM IP's Management capabilities
15	Shall distribute data intelligently across all nodes and capacity utilization across all nodes has to be uniform at all times.
16	Shall be capable of adding additional combined server and storage components with high performance GPU capabilities, seamlessly, with no downtime, to scale performance and capacity on demand
17	Native storage level snapshots with no impact to guest performance or using any additional storage capacity
18	The solution should support data replication with disk space optimization
19	The platform should have capability to leverage SSD for IOPS hungry workload should be running from SSD only
20	The platform should have support for rack /chassis awareness to support redundant data should go to different rack/chassis nodes
21	The proposed HCI should support native File Services over NFS/CIFS/SMB and file replication across clusters and data centers

22	The proposed HCI solution must provide operations management and provide performance, storage, CPU utilization per VM
23	Platform must provide management through a web based HTML 5 console. Must provide storage, compute & hypervisor metrics on a per VM level as well as health and monitoring of entire platform. Platform should support LDAP Active Directory integration
24	Platform must support monitoring via SNMPv3 and email alerting via SMTP
25	Shall be capable of creating instant snapshots of virtual machines and maintaining multiple copies of snapshots & clones
26	Proposed HCI solution should support fault tolerance of at least two nodes failure within a cluster
27	Solution must support native VM level replication for installed Hypervisor
28	The solution should have call home capability for remote log collection and proactive support for predictive failure hardware component
29	Proposed HCI solution should have inline deduplication and compression for the proposed capacity
30	The proposed solution should provide a minimum of 200TB of usable storage. Any additional storage required for successful solution deployment should be considered and provided by the bidder.

Enterprise Management System

S.No.	Component	Description
1	**SLA & Contract management System**	▪ 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

S.No.	Component	Description
		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 KICCC Project under discussion. ▪ The solution should support requirements of the auditors requiring technical audit of the whole system which MSI should allow the auditors to access the 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. 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 KICCC 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.

S.No.	Component	Description
		• The solution must support Templates for report generation, Report Filtering and Consolidation and Context sensitive Drill-down on specific report data to drive standardization and governance of the KICCC project • The solution must support security for drill-down capabilities in dashboard reports ensuring visibility for only relevant personnel of the KICCC project • Support real-time reports (like at-a-glance status) as well as historical analysis reports (like Trend, TopN, Capacity planning reports etc.)
2	**Network Monitoring System**	▪ The Solution should provide capability to monitor any device based on SNMP v1, v2c & 3 ▪ The Solution should monitor bandwidth utilization. ▪ The solution should monitor utilization based on bandwidth ▪ The Solution must be capable of monitoring the availability, health, and performance of core networking devices including but not limited to CPU, memory, temperature. ▪ The Solution should have the ability to issues pings to check on availability of ports, devices. ▪ The Ping Monitoring should also support collection of packet loss, Latency and Jitters during ICMP Ping Checks ▪ The Port Check for IP Services monitoring should also provide mechanism to define new services and ability to send custom commands during port check mechanism. ▪ The Solution should have the ability to receive SNMP traps and syslog. ▪ The Solution should automatically collect and store historical data so users can view and understand network performance trends. The solution should be capable of monitoring network delay/latency. ▪ The solution should be capable of monitoring delay variation ▪ The solution should be capable of monitoring packet loss, Packet QOS, Packet Errors on one or more ports ▪ The solution should allow users to access network availability

S.No.	Component	Description
		and performance reports via the web or have those delivered via e-mail. ▪ The solution should support auto-discovery of network devices ▪ The solution should have the ability to schedule regular rediscovery of subnets. ▪ The solution should provide the ability to visually represent LAN/WAN links) with displays of related real-time performance data including utilizations. ▪ The system should provide discovery of heterogeneous physical network devices like Layer-2 & Layer-3 switches, Routers and other IP devices and do mapping of LAN & WAN connectivity. ▪ The System shall support monitoring of Syslog ▪ The solution should provide capability to add an IP device or IP Range or IP subnet with functionality supporting multiple SNMP strings. ▪ The solutions should have real time, detect configuration and asset information changes made across a multi-vendor device network, regardless of how each change is made and also support configuration deployment/rollback and configuration templates.
3	**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, utilization, and performance in order to measure central SLA's and calculate penalties

S.No.	Component	Description
5	**Application Performance Management**	▪ The solution should measure the end users' experiences based on transactions without the need to install agents on user desktops. ▪ The solution must be able to provide user usage analysis and show how user's success rate, average time and transaction count has changed over a specific period of time such as current week versus previous week. ▪ The solution must be able to provide the ability to detect and alert when users experience HTTP error codes such as 404 errors or errors coming from the web application. ▪ Solution shall be able to monitor customer transaction by end-user name, and thus able to understand exactly which customers were impacted, their location, type of browser used etc. ▪ The solution must simplify complex app topologies through task–relevant views based on attributes such as location, business unit, application component etc. ▪ The solution must speed up the process of triage by showing the impact of change, thus enabling to easily locate where performance problems originate. The solution should provide the flexibility of collecting deep-dive diagnostics data for the transactions that matter for triage as opposed to collecting deep-dive data for every transaction. ▪ The solution must proactively monitor 100% of real user transactions; detect failed transactions; gather evidence necessary for triage and diagnosis of problems that affect user experiences and prevent completion of critical business processes. ▪ The solution must determine if the root cause of performance issues is inside the monitored application, in connected back-end systems or at the network layer from a single console view. ▪ The solution must provide proactive real-time insights into real user behavior, trends, log analytics and performance to enhance customer experience across various channels ▪ The solution must provide operational efficiency capabilities

S.No.	Component	Description
		that provide insight of app performance by version, geo, OS, network, real-time alerts on threshold violations impacting SLAs and prioritize alerts based on impact to business, revenue and gain end- to-end visibility into the mobile infrastructure. ▪ The solution must provide complete Insights into Application Flows, Heat Maps to enable improving the UI design, understand user interactions, build functionality based on real user data and create product & services differentiation.
6	**Asset Management System**	▪ Ability to provide inventory of hardware and software applications on end-user desktops, including information on processor, memory, OS, mouse, keyboard, etc. through agents installed on them. ▪ Ability to have reporting capabilities; provide predefined reports and ability to create customized reports on data in the inventory database. Report results could be displayed as lists or graphs. ▪ Ability to provide the facility to collect custom information from desktops. ▪ Ability to provide facility to recognize custom applications on desktops. ▪ Facility for the administrator to register a new application to the detectable application list using certain identification criteria. Shall enable the new application to be detected automatically next time the inventory is scanned. ▪ Ability to support configuration management functionality using which standardization of configuration can be achieved of all the desktops. ▪ Software metering shall be supported to audit and control software usage. Shall support offline and online metering. ▪ Ability to support dynamic grouping of enabling assets to be grouped dynamically based on some pre-defined criteria e.g. a group shall be able to display how many and which computers has a specific application installed. As and when a new computer gets the new application installed it shall dynamically add to the group.

S.No.	Component	Description
		▪ Ability to use the query tool to identify specific instances of concern like policy violation (presence of prohibited programs / games and old versions, etc.), inventory changes (memory change, etc.) and accordingly it could perform several actions as reply. These actions may be (a) sending a mail, (b) writing to file (c) message to scroll on monitor screen, etc. ▪ Facility to track changes by maintaining history of an asset. ▪ The proposed EMS solution shall provide comprehensive and end -to-end management of all the components for each service including all the hardware devices, Network, Systems and Application infrastructure. Note: It is mandatory that all the modules for the proposed EMS Solution shall provide out-of-the-box and seamless integration capabilities. SI shall provide the specifications and numbers for all necessary Hardware, OS & DB (if any) which is required for an EMS to operate effectively.

Backup/Replication/Archival Solution

Backup Solution Requirements

S.No.	Description
1	The proposed backup solution shall have same GUI across heterogeneous platform to ensure easy administration and available on various OS platforms such as Windows, Linux and UNIX platforms and be capable of supporting backup/ restores from various supported platforms.
2	Backup Solution should have ability to backup data from one server platform and restore it to another server platform to eliminate dependence on a particular machine and for disaster recovery purposes.
3	Backup Solution should support various level of backups including full, incremental, and user driven backup along with various retention period.
4	Backup clients should be updated automatically using the client push feature
5	Backup should support agentless backup for virtualization platform with non-

S.No.	Description
	staged granular recovery.
6	Backup Software should support intelligent policy for virtualization.
7	Backup Software must provide Source (Client & Media Server) & Target base data Deduplication capabilities.
8	Backup Solution should Integrate with third party VTL, NAS, SAN which has data deduplication capabilities and Robotic/automated Tape library
9	Backup Solution must have Wizard-driven configuration and modifications for backup, restoration and devices.
10	The proposed backup solution shall have in-built frequency and calendar based scheduling system.
11	Backup Solution must have Optimized way for data movement from client to disk target.
12	Backup Solution should support (inflight & at rest) encryption.
13	The proposed backup solution shall support tape mirroring of the same job running concurrently with primary backup.
14	The proposed backup solution shall allow creating tape clone facility after the backup process.
15	Backup Solution should have Capability to do trend analysis for capacity planning of backup environment.
16	The proposed Backup Solution must offer capacity-based licensing. The license should be for the front-end capacity rather than back-end. There should be no incremental cost associated with longer retention periods.
17	The solution should not require purchase of additional licenses for DR sites (copies of original data), also should not require purchase of additional licenses for replication to DR sites.
18	The proposed backup solution license should be independent of hardware so replacing hardware should not incur new software license cost.
19	The proposed backup solution must include Agent/Modules for online backup of files, applications and databases.
20	The proposed backup solution should provide recovery from physical servers to Virtual and image level recovery.
21	The proposed backup solution should have Cloud plug-ins for backup data replication.
22	Backup Solution should have Inbuilt feature for extensive alerting and reporting

S.No.	Description
	with pre-configured and customizable formats.
23	Backup Replication at DR site, Cloud. Replication license should be included as part of solutions.
24	Backup software should support multiplexing and multi-streaming and shall support the capability to write up to Min 32 data streams.
25	Backup Solutions should have capabilities to tape/disk out backup catalog and deduplication catalog.
26	Backup solution should have integrated data de-duplication engine with multi-vendor storage support to save de-duplication data. The de-duplication engine should also facilitate IP base replication of de-dupe data; without any extra charge.
27	The Proposed Backup solution must be capable of restoring files, emails and other granular items from different applications for e.g. File Exchange Server, Active Directory etc. and for hypervisors, virtualisation softwares etc. from a single-pass backup.
28	Backup solution must Support Backups/Restores for 1) Clustered servers (Industry popular clusters). 2) Virtual platform. 3) RAW SCSI volumes. 4) Block based backup & restore simultaneously.

Replication Solution

S.No.	Description
1	The proposed architecture should ensure that in event of Disaster at Primary Site, applications can be restarted at DR Site without any data loss.
2	The proposed architecture should focus on not only the data replication, but ensuring application availability with zero data loss at DR site.
3	The proposed solution must optimize additional infrastructure and storage resources in the architecture.
4	The proposed solution should be a storage agnostic solution. The solution should not only seamlessly integrate with current infrastructure, but also not impose any restriction on storage or platform technology that VSCL may deploy in future.
5	The proposed software must provide comprehensive hardware and platform

S.No.	Description
	support. Support for physical and virtual platforms.
6	The proposed software should provide application level availability by ensuring that it not only replicates data within database but also structural changes to databases, application and database binaries etc. without any manual intervention.
7	Application high availability at primary & DR site should not be dependent on Operating system event logs. Solution should be capable to integrate directly with application start, stop and monitor service to avoid outage remedy solution because of Operating system log.
8	The proposed software should support real time tracking of configuration changes being done to Operating system, application binaries, any tunable added/modified etc. and alert administrators in case of configuration drift between primary and DR site.
9	Shall be able to handle long outages of network without affecting the consistency of data at secondary site. The replication solution should be provisioned for storing data for at least 4 days in case network is down for extended period.
10	The proposed software should provide for an automated fire-drill for testing of DR site. The testing mechanism should automatically validate the application start up at DR site at a pre-defined schedule defined.
11	The proposed software should provide availability across any distance—Builds local metropolitan and wide-area clusters for disaster recovery and local availability.
12	The proposed software should ensure no single point of failure. It has the ability to gracefully move an application to an available server in the event of a failure and coordinate the movement with storage ownership.
13	The proposed software should provide Multi-cluster management and reporting, including applications composed of multiple components running on different physical and virtual tiers, adding resilience to business services. Manages and reports on multiple local and remote clusters from a single unified web-based console.
14	The proposed software should provide seamless integration with all applications/databases used for increased application performance and availability.
15	It should also have the integration capability with replication softwares/technologies.

S.No.	Description
16	The proposed software should provide advanced application failover logic to ensure that application uptime is maximized, server resources are efficiently utilized, and detect failures faster than traditional clustering solutions and requires almost no CPU overhead
17	The proposed software should provide advanced clustering support for virtual machine architectures.
18	The proposed software should be simple to install, configure, and maintain. It should provide powerful wizards that enable simple, quick, and error-free setup of advanced, high availability, disaster recovery, and Fire Drill configurations.
19	The proposed software must be able to provide comprehensive insight into the storage environment, enabling improved usage and efficiency across all major operating systems and storage hardware.
20	The proposed software should have deduplication and compression to reduce the primary storage footprint.
21	The proposed software should support automated storage tiering to seamlessly and transparently move data based on business value
22	The proposed software should have the ability to make data compatible between operating systems for simplified OS migration.
23	The proposed software should be able to support physical environment. It should support virtual disks in VMDK/VMFS format, and as well as RDM.
24	The proposed solution should have multi-pathing feature for I/O path availability and performance to efficiently spread I/Os across multiple paths for maximum performance, path failure protection, and fast failover.
25	Host Replication should be certified for performing replication to heterogeneous storage models from different.
26	The Host Replication technology should support different types of data whether structured or unstructured.
27	The proposed host base replication solution should be capable of maintaining data consistency at all times.

Archival Solution

S.No.	Description
1	The solution must be capable of archiving content from multiple sources like messaging including File Servers , VOIP etc.

S.No.	Description
2	The proposed solution must have integration with Email solution through SMTP archiving without the need of any additional hardware.
3	The solution should have the capability to archive data from multiple electronic repository to single repository to achieve best single instance across multiple frontend source data.
4	The solution must support a Single unified console to manage archiving from different sources like File server, Mailing solution etc.
5	The solution should provision a web based discovery mechanism to search relevant data across archives from multiple sources like file server, messaging etc. The discovery mechanism should support a guided, hierarchal review of searched data with capability to filter, marking and legal hold to prevent deletion/expiry.
6	The solution should facilitate a supervision mechanism for emails to ensure compliance of messaging content. The supervision mechanism should facilitate sampling of messages and subsequent review by authorized personnel
7	The solution should support tagging of messages by message security solutions like anti-spam/anti-virus for efficient retention
8	Proposed solution must support outlook on Windows & MAC machines.
9	Archival solution must have support with IMAP compliant devices to access the emails.
10	Proposed solution should support archiving both at premises and cloud.
11	Proposed solution must have monitoring integration with messaging solution vendor.
12	The solution should support Message Journaling as well as Envelope Journaling, capture data and expansion of distribution lists
13	The solution must support "Agentless" archiving of messages. There should be no need to deploy any agent on the messaging server.
14	The solution must support search for mails based on undisclosed recipients criteria
15	The solution should support seamless access using shortcuts from the native email client as well as browser based client. The solution should support all archiving actions like manually archive, search, restore, retrieve, delete from the native email client and browser based client

S.No.	Description
16	The solution should support archiving based on either any or a combination of the following criteria: • Item Type (message, calendar etc.) • Date • Size • Email Attachment only • User • Organizational Unit
17	Proposed solution must have advance way of archive disk/partition data backup to avoid backup of old partitions which must be possible with or without WORM devices.
18	The solution must allow the administrators to configure the following in shortcuts: • Include recipient information in the shortcuts. • Include nothing / original message body / custom message body in shortcuts. • Include "X" number of characters in the shortcut. • Include a custom body defined from a configuration file in the shortcut etc.
19	The solution should leave a shortcut at either the time of archiving or later as well.
20	The solution should allow users to view archived items directly without having the need to restore them to the messaging server to avoid delays and impact on messaging solution. No network connections should be established between archiving server and messaging server at the time of retrieving archived items
21	The solution must support indexing and archiving of minimum 500+ commonly used file types.
22	The solution should support archiving of entire email folders and application of selective archiving policies based upon folders.
23	The solution must support dynamic retention period of archived items i.e. retention of archived items can be increased or decreased on fly.
24	The solution should facilitate "future proofing" of content by facilitating an HTML copy for long term retention and search
25	The solution should support "safety copies" of items to be kept on the mail server. The "safety copy" allows the archiving software to wait for the archived item to be backed up or replicated before the original item is removed from the

S.No.	Description
	mail server.
26	Archival solution must have option to set or configure disk property read and read-write access
27	Archival solution must have disk configurable option with High & Low watermark. In case, High watermark reaches, disk should automatically become Read only and other pre-configured disk should get read-write access to store fresh archived items.
28	The solution must have OWA integration in such a fashion that archived item can be browsed directly through archived browser tab instead of browsing through internet explorer (IE). IE can be additional feature.
29	The archival solution must have an integrated e-discovery solution which allows guided Discovery, review and analysis of data from the archives and non-archived data like desktop, file server, Documentum etc. It's required for future proofing.
30	Proposed Archival solution must have seamless and consistent end user search experience across multiple interface like Desktop/Laptop, mobile, tablets etc.

Server Infrastructure Zone

This zone shall host servers, server racks, storage racks and networking components like routers, switches to passive components. All the Data center LAN connections shall be provided through switches placed in this area. MSI shall be required to undertake a detailed assessment of the space and size of the building proposed by client for KICCC with co-hosted data center with respect to their system requirements and if required may propose a suitable solution. Access to this zone, where the surveillance project IT infrastructure is hosted, shall be demarcated and physical access to the place shall be given only to the authorized personnel. Indoor CCTV Cameras shall be installed to monitor the physical access of the system from remote location.

UPS and Electrical Zone

This zone shall house all the Un-Interrupted Power Supply units, Main Power Distribution Units (PDUs) to feed the components such as PAC, UPS, lighting, fixtures etc. This shall also house all the batteries accompanying the UPS components. As these generate good amount of radiation, it is advised to house these components in a room separate from server infrastructure zone.

Technical Specifications- DC/ DRC:

Web Security Appliance:

Sr. No.	Technical Specification	Minimum Requirements
1	**Appliance Requirement and Functionality**	The solution should be a hardened Web Proxy, Caching, Web based Reputation filtering, URL filtering, Antivirus and Anti-malware appliance. All the functionalities should be in a single appliance only.
2	**Hardware**	Minimum of 1 * 6-core CPUs, 2.4 TB storage, RAID 10, 32 GB or more DRAM, hot-swappable hard drive
3	**Operating System**	The appliance based Solution should be provided with hardened Operating System.
4	**Operating System Performance**	The underlying operating system and hardware should be capable of supporting atleast 2000 users from day with licenses & scalable upto 5000 users.
5	**Operating System Security**	The operating system should be secure from vulnerabilities and hardened for web proxy and caching functionality.
6	**IP V6 Support**	Should have the ability to proxy, monitor, and manage IPv6 traffic.
7	**Forward proxy mode**	The solution should support explicit forward proxy mode deployment in which client applications like browsers are pointed towards the proxy for web traffic.
8	**Proxy support**	The proposed solution should be a Fast Web Proxy and should support HTTP, FTP and HTTPS proxy.
9	**HTTPS Decryption**	The solution should support HTTPS decryption
10	**HTTPS decrypted traffic scanning**	The solution should support scanning of the https decrypted traffic by the on-board anti-malware and/or anti-virus engines.
11	**HTTPS decryption policy**	HTTPS decryption should provide flexibility to have multiple decryption policies and should not be just a Global action

Sr. No.	Technical Specification	Minimum Requirements
12	**Proxy Chaining**	The solution should support proxy configuration in a Chain. The Lower end proxies at spoke locations should be able to forward the request to an Higher end proxies at Hub Location forming a Chain of Proxies
13	**DNS Splitting**	The solution should support configuration to use Split DNS. It should be able to refer to different DNS for Different Domains e.g. (root dns for all external domains and internal DNS for organization domain
14	**IP Spoofing support in transparent mode deployments**	The solution should have facility to do IP spoofing. When enabled, requests originating from a client should retain the client's source address and appear to originate from the client instead of the appliance. This is useful in scenarios where policies are based on original IP and logging/reporting is required to track activity of individual IP basis.
15	**Transparent mode**	The solution should also support transparent mode deployment using WCCP v2 and L4 switches/PBR (Policy-based Routing)
16	**Pac File support**	The appliance should support hosting proxy auto-config files that defines how web browsers can automatically choose the appropriate web proxy for fetching a URL.
17	**Support multiple deployment options**	The solution should allow to deploy the appliance in explicit proxy as well as transparent mode together.
18	**Remote support**	The remote support from principal company should be available via India Toll Free and Email. The Support Portal access should be provided for Case management, knowledgebase, new version information, tools etc.
19	**Secure Remote Access**	The Support Engineers should be able to login to appliance using secure tunneling methods such as SSH for troubleshooting purposes
20	**High Availability**	Provision of active/active High Availability is required

Sr. No.	Technical Specification	Minimum Requirements
21	**Application and Protocol Control**	The solution should support granular application control over web eg. Facebook controls like block file upload, block posting text, enforcing bandwidth limits on application types.
22	**File download and size restrictions**	The solution should be capable of blocking specific files downloads and based on size and per user group basis. It should also provide option to block object using MIME File types.
23	**IP based Access Control**	The solution should allow administrator to define access to internet based on IP addresses, range of IP addresses, subnet and CIDR basis. It should also support to be forced for Authentication from Specific IP addresses, Subnet or CIDR's
24	**User based Access Control**	The solution should support integration with active directory and/or LDAP. This should allow administrator to define user or group based access policies to Internet
25	**Multiple Authentication Server Support**	The solution should support Multiple Auth Servers / AuthFailover using Multi Scheme Auth (NTLM and LDAP). It should also support authentication exemption.
26	**Layer 4 Traffic Monitoring**	Should detect Phone Home attempts occurring from the entire Network. It should support actions to allow traffic to & from known malware addresses & should support from known allowed & unlisted addresses & block traffic to & monitoring suspected malware addresses.
27	**Bandwidth restrictions**	The solution should support providing bandwidth limit/cap for streaming media application traffic. This should be possible at the Global level as well as at a per policy level.

Sr. No.	Technical Specification	Minimum Requirements
28	**Anti Malware**	The appliance should support at least 2 industry known Anti Malware/Anti-Virus engine that can scan HTTP, HTTPS and adware, browser hijackers, phishing and pharming attacks to FTP traffic for web based threats, that can range from more malicious threats such as rootkits, Trojans, worms, system monitors and Keyloggers and as defined by the organizations policy. Please mention the antimalware engine.
29	**Malware Protection**	With dual AV/Anti-Malware engine scanning when a URL causes different verdicts from the scanning engine the appliance should perform the most restrictive action.
30	**Web Reputation**	The solution should provide Web Reputation Filters that examine every request made by the browser (from the initial HTML request to all subsequent data requests) – including live data, which may be fed from different domains to assign a web based score to determine the likelihood that it contains url-based malware.
31	**Customizable Web Reputation**	The Appliance should have customizable setting in the Web Based Reputation Services, like Allow, Scan and Block based on the scoring settings by the Administrator.
32	**Incoming/Outgoing Traffic scanning**	The solution should scan for Incoming and outgoing traffic.
33	**Outbound connection control on all ports and protocols**	The solution shall provide option to scan all ports at wire speed, detecting and blocking spyware activity trying to connect to the outside Internet. By tracking all 65,535 network ports and all protocols, the solution shall effectively mitigate malware that attempts to bypass Port 80
34	**Custom URL filtering**	The solution should support creation of custom URL categories for allowing/blocking specific destinations as required by the Organisation.

Sr. No.	Technical Specification	Minimum Requirements
35	**URl Filtering Options**	The web Proxy should support following actions like allow, monitor, block, time-based access. Should also support displaying a warning page but allows the user to continue clicking a hypertext link in the warning page.
36	**URL check & submission**	Support portal should give facility to end user to check URL category and submit new URL for categorization
37	**Dynamic Categorization**	Provision should be available to enable Real Time Dynamic categorization that shall classify in real time in case the URL the user is visiting is not already under the pre-defined or custom categories database.
38	**Reporting Mis-categorization**	The solution should have facility for End User to report Mis-categorisation in URL Category.
39	**Filtering Content**	Solution should support filtering adult content from web searches & websites on search engines like Google.
40	**Signature based application control**	The solution should support signature based application control.
41	**End User Notification**	Solution should support following end user notification functionalities. The proxy should support the functionality to display a custom message to the end user to specify the reason the web request is blocked.
		When the website is blocked due to suspected malware or URL-Filters it should allow the end user to report that the webpage has been wrongly misclassified.
		The solution should support the functionality of redirecting all notification pages to a custom URL to display a different block page for different reasons.
		Should support the functionality to force users to explicitly agree to the terms and conditions for browsing the World Wide Web from the organization's network to let the user know that the Organisation is monitoring their web activity.
42	**Diagnostic Tools**	The appliance should have diagnostic network utilities like telnet, traceroute, nslookup and tcpdump/packet capture.

Sr. No.	Technical Specification	Minimum Requirements
43	**Updates and Upgrades**	The appliance should provide seamless version upgrades and updates.
44	**Secure Web Based management**	The appliance should be manageable via HTTP or HTTPS
45	**CLI based management**	The appliance should be manageable via command line using SSH
46	**Serial Console access**	For emergency, the appliance should have serial console access
47	**Ethernet Management**	Should have provision for separate Ethernet for managing the appliance
48	**Web Logs**	The Proxy Log should be scalable. The log formats shall include Apache, Squid and W3C.
49	**Retention Period**	The retention period should be customizable. Options should be provided to transfer the logs to an FTP using FTP or SCP.
50	**User Reports**	Informative and exhaustive set of reports on User Activity and URL filtering activities (GUI to report past activity, top usage users and top malware threat)
51	**Bandwidth Reports**	Reports on Bandwidth Consumed / Bandwidth Saved
52	**Detailed logging**	Product to maintain detailed proxy access logs that can be searched via filters, for easy location of any desired access of the user and to see how the product dealt with it
53	**Blocked by reputation &malware reports**	It should support reporting web requests blocked due to web reputation & blocked by malware
54	**Report Formats**	Solution should support generating a printer-friendly formatted pdf version of any of the report pages. Should also support exporting reports as CSV files.
55	**Scheduling of Reports**	Solution should support to schedule reports to run on a daily, weekly, or monthly basis.
56	**System Reports**	Should support system reports to show CPU usage, RAM usage, percentage of disk space used for reporting & logging.

Sr. No.	Technical Specification	Minimum Requirements
57	**Updates and Upgrades**	Support should cover all upgrades for the time period the licenses and support purchased from principal vendor

Anti-APT Feature

Sr. No.	Specifications
1	Anti-APT solution should be appliance based and should offer a minimum throughput of 2 Gbps
2	Appliance should support at least 8*1Gbps ports
3	Appliance shall provide a separate management port and should also provide a web-based GUI management
4	Appliance should provide at least 10000 concurrent users
5	Appliance should be capable of working in Inline Blocking mode without depending on other network components like a separate FW, IPS or Web Security Appliance
6	Appliance should have fail-open capabilities for all ports
7	Appliance should have dual hot-swappable power supplies
8	Solution should be capable of blocking call backs to CnC Servers
9	Solution should be capable of blocking threats based on both signatures and behaviour
10	Proposed solution's detection rules should be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.
11	Proposed solution should be capable of blocking threats on the following protocols: HTTP, HTTPS
12	The solution should be capable of executing MS Office Documents, Portable Documents, Archive Files, Multimedia Files and executable binaries in a virtual sandbox environment
13	The solution should be capable of exempting specific hosts from specific compliance rules and suppressing corresponding compliance events and alerts.

14	The solution should be capable of gathering Active Directory user identity information, mapping IP addresses to username and passively gathering information about network devices including but not limited to:
	• Network protocols used, e.g. IPv6, IPv4
	• Network services provided, e.g. HTTPS, SSH
	• Open ports, e.g. TCP:80
	• Client applications installed and type, e.g. Chrome - web browser
	• Web applications access, e.g. Facebook, Gmail
	• Risk and relevance ratings should be available for all applications
	• Potential vulnerabilities
	• Current User
	• Device type, e.g. Bridge, Mobile device
	• Files transferred by this device/user
15	The solution should be capable of whitelisting trusted applications from being inspected to avoid business applications from being affected & in turn productivity
16	The solution should be capable of blocking traffic based on geo locations to reduce the attack landscape and to protect communication to unwanted destinations based on geography
17	The sandbox should be appliance based with the ability to run multiple versions of 32 and 64-bit client and Server Windows within the same environment
18	All the devices shall be managed centrally and should be capable of
	• Centralized, life cycle management for all sensors
	• Aggregating all events and centralized, real-time monitoring and forensic analysis of detected events
	• Must provide a highly customizable dashboard
19	The sandbox should be appliance based with the ability to run multiple versions of Windows within the same environment
20	The Sandbox should be a proprietary custom-built malware analysis solution and not open source or generic sandbox
21	The Sandbox should be a proprietary custom-built malware analysis solution and not open source or generic sandbox and should provide:
	- analysis reports
	- threat score of the sample
	- ability to queue samples,
	- impact analysis

	- Global Threat Intelligence
	Sandbox shall be able to detect memory residing malware
22	The proposed solution shall have the capability to continuously track a file's disposition based on global intelligence and do a retrospective block and alert if the file has exhibited malicious traits globally even if the file hasn't started behaving maliciously locally
23	The solution should include protection against desktop and server & should support minimum Windows 7 desktop, Windows server 2003 & 2008. Bidder should provide license for 1000 window based PC/Servers.

Servers

S.No.	Item	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 The required connectivity can be provided using converged FCOE ports on Blade servers
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

Blade Chassis Specifications

The blade chassis shall have the following minimum technical specifications:

- Minimum 6U size, rack-mountable, capable of accommodating minimum 8 or higher hot pluggable blades

- Dual network connectivity of 10 G speed for each blade server for redundancy shall be provided
- Backplane shall be completely passive device. If it is active, dual backplane shall be provided for redundancy.
- Have the capability for installing industry standard flavors of Microsoft Windows, and Enterprise RedHat Linux Oss as well as virtualization solution.
- 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
- Minimum 1 USB port
- Two hot-plug/hot-swap, redundant 10 Gbps Ethernet or FCoE module with minimum 16 ports (cumulative), having Layer 2/3 functionality
- Two hot-plugs / hot-swap redundant 16 Gbps Fiber Channel or FCoE module for connectivity to the external Fiber channel Switch and ultimately to the storage device
- Hot plug/hot-swap redundant power supplies to be provided, along with power cables
- Power supplies shall have N+N. All power supplies modules shall be populated in the chassis.
- Required number of PDUs and power cables, to connect all blades, Chassis to Data Center power outlet.
- Provision of systems management and deployment tools to aid in blade server configuration and OS deployment
- Blade enclosure shall have provision to connect to display console/central console for local management such as troubleshooting, configuration, system status/health display.
- 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.
- The chassis shall be able to support redundant modules for fabric connectivity
- Each port should be able to carry the traffic of multiple VLANS.
- The power supply modules should be hot pluggable
- Power supply should meet the Energy 80 Plus certification
- Should be configured to provide full redundant cooling to all blade slots
- It should suport remote KVM capability from an external keyboard, video monitor and mouse to all blades installed in the chassis through the management controller.
- Simultaneous KVM access to a single blade KVM by multiple users but the admin user can take Read Write ownership while the other user is in Read Only mode

Firewall with IPS & URL Filtering:

Sr. No.	Specifications
1	**Hardware Architecture**
	The appliance-based security platform should be capable of providing firewall, application visibility, and IPS functionality in a single appliance
	The appliance should support at least 2 * 10G ports scalable upto 8x10G, the firewall should be modular in nature so that it can be scalable 2 * 40G ports in future
	The appliance hardware should be a multicore CPU architecture with a hardened 64-bit operating system to support higher memory
	Proposed Firewall should not be proprietary ASIC-based in nature & should be open architecture based on multi-core CPU's to protect & scale against dynamic latest security threats.
2	**Performance & Scalability**
	Should support at least 10 Gbps of production performance / multiprotocol combined firewall & IPS throughput
	Firewall should support at least 8,000,000 concurrent sessions
	Firewall should support at least 60,000 connections per second
	Firewall should support at least 1000 VLANs
3	**Firewall Features**
	Firewall should provide application detection for DNS, FTP, HTTP, SMTP,ESMTP, LDAP, MGCP, RTSP, SIP, SCCP, SQLNET, TFTP, H.323, SNMP
	Firewall should support creating access rules with IPv4 & IPv6 objects simultaneously
	Firewall should support operating in routed & transparent mode
	Should support Static, RIP, OSPF, OSPFv3 and BGP
	Firewall should support manual NAT and Auto-NAT, static nat, dynamic nat, dynamicpat
	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to-IPv6) functionality
	Firewall should support Multicast protocols like IGMP, PIM, etc.
	Should support security policies based on security group names in source or destination fields or both
	Should support capability to limit bandwidth on basis of apps/groups, Networks / Geo, Ports, etc.
	High-Availability Features

Sr. No.	Specifications
4	Firewall should support Active/Standby failover
	Firewall should support ether channel or equivalent functionality for the failover control & date interfaces for providing additional level of redundancy
	Firewall should support redundant interfaces to provide interface level redundancy before device failover
	Firewall should support 802.3ad Ether channel or equivalent functionality to increase the bandwidth for a segment.
	Firewall should have integrated redundant power supply
	Firewall should have redundant hot-swappable FANs
5	**Next Generation IPS**
	Should have the capability of passively gathering information about virtual machine traffic, network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.
	Should be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.
	Should be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports.
	Should be able to link Active Directory and/or LDAP usernames to
6	**IP addresses related to suspected security events.**
	Should be capable of detecting and blocking IPv6 attacks.
	Should support the capability to quarantine end point
	The solution should support full-featured NBA capability to detect threats emerging from inside the network. This includes the ability to establish "normal" traffic baselines through flow analysis techniques (e.g., NetFlow) and the ability to detect deviations from normal baselines.
	The solution must provide IP reputation feed that comprised of several regularly updated collections of poor reputation of IP addresses determined by the proposed security vendor
	The solution must support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist.
	Should must support URL and DNS threat feeds to protect against threats
	Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies on more than 280

Sr. No.	Specifications
	million of URLs in more than 80 categories.
	The solution must be capable of passively gathering details unique to mobile devices traffic to identify a wide variety of mobile operating systems, mobile applications and associated mobile device hardware.
	Should support more than 4000 application layer and risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.
	Must be capable of providing network-based detection of malware by checking the disposition of known files in the cloud using the SHA-256 file-hash as they transit the network and capability to do dynamic analysis on- premise (if required in future) on purpose built appliance
	The Appliance OEM must have its own threat intelligence analysis center and should use the global footprint of security deployments for more comprehensive network protection.
	The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).
	Should be able to identify attacks based on Geolocation and define policy to block on the basis of Geo-location
	The detection engine should support the capability of detecting variants of known threats, as well as new threats
	The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioral anomaly detection techniques. Identify and explain each type of detection mechanism supported.
	Should support Open based application ID for access to community resources and ability to easily customize security to address new and specific threats and applications quickly
	The integrated solution should also provide URL filtering functionality for upto 200 million URL's, upto 60 different categories for URL
	Management
7	The management platform must be accessible via a web-based interface and ideally with no need for additional client software

Sr. No.	Specifications
	The management platform must provide a highly customizable dashboard.
	The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows
	The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.
	Should support REST API for monitoring and config programmability
	The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.
	The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).
	The management platform must provide robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.
	The management platform must risk reports like advanced malware, attacks and network
	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools.

Internet and Aggregation Router

Sr. No.	Specifications
1	Router should be chassis based device with minimum 10 Gbps of throughput scalable upto 20 Gbps. It should have minimum 4 GB of RAM/ DRAM
2	Router supports management protocol: SNMP v1/v2/v3, CLI (Telnet/Console), TFTP update and configured file management
3	Router must have inbuilt state full firewall, zone-based firewall and 3 DES capability technologies to support the access controller strategy based source and destination IP protocol port and time parameters
4	Router should have tunneling protocols like IPsec VPN, GET VPN or equivalent, Multi Point VPN and encryption mechanisms like DES, 3DES, AES (128 and 256Bit).It should support minimum 300 IPsec tunnels from day one.

Sr. No.	Specifications
5	Router has support for the following routing /WAN protocols
6	PPP/MLPPP, HDLC
7	Router should be modular chassis based device and should accommodate a combination of high-density Sync / Async Serial, 10G, Gigabit Ethernet, Fast Ethernet
8	Router should support protocols like RIP, OSPF, BGP, VRRP/HSRP, 802.1q, GRE, ACL's and NAT MPLS, traffic engineering, EoMPLS or VPLS
9	or equivalent, L2 VPN from day one
10	Shall support the RIPng & BGP for IPv6, OSPFv3, MPLS, BGP from day one.
11	Router should have 18000 route support from day one
12	The router supports state full packet inspection supporting H.323, SIP and other application level gateway support
13	The state full firewall supports IPsec pass through
14	The router/ System shall support of classifying applications based on the category they belong to (For e.g. file sharing, voice, video-conferencing, business-tools etc.) from day one. System shall support of support customized categories for their applications, help identify distinctly the voice and video streams in the network from day one.
15	System shall support to provide the ability to filter and gather application information in a flexible manner from day one
16	Router should support QoS Classification and marking policy based routing, IP precedence, DSCP
17	QoS -congestion management WRED/RED, Priority queuing, class-based weighted for fair queuing
18	IP Access list to limit Telnet SNMP access to router
19	Multiple privilege level authentication for console and telnet access
20	Time-based ACL for controlled forwarding based on time of day for offices
21	Should have extensive support for SLA monitoring for metrics like delay latency, jitter, packet loss and MoS
22	Provides QoS features like traffic prioritization, differentiated services, and committed, and committed access rate, QoS Support, RSVP/WFQ/MRED. Router should be able to take pre-configured action on these events like changing routes, changing routing metric
23	Router supports for QoS Features for defining the QoS policies. Support for low latency queuing, Layer 2 and Layer 3 CoS/DSCP

Sr. No.	Specifications
24	Router should have multicast routing protocols support: IGMPv1, v2 (RFC2236) PIM-SM (RFC2362) and PIM-DM/ Multicast VLAN Registration
25	The following interface required from Day-1: 2x 10G SFP+ based ports loaded with single mode transceiver, 3*1GE & 3*1G SFP-based transceiver.
26	The router should be IPv6 ready

L2 PoE Switch

Sr. No.	Specifications
1	19" Rack Mountable stackable switch with min 24 Nos. 10/100/1000 copper input POE (15.4W) ports and additional support of 4x1G SFP, support for external/internal redundant power supply.
2	Switch should support for minimum 96 Gbps of forwarding throughput & minimum 70 mpps forwarding rate
3	The switch should support dedicated stacking port separate from uplink ports with 80 Gbps of stacking bandwidth to put minimum 8 switches into a single stack group.
4	Switch should have static, default IP routing enabled from day one.
5	Switch shall have IEEE 802.3ad Link Aggregation Control Protocol (LACP) with up to 8 links (ports) per trunk.
6	It shall have IEEE 802.1s Multiple Spanning Tree Protocol and provide legacy support for IEEE 802.1d STP and IEEE 802.1w RSTP or equivalent technology and static routes.
7	Switch should have feature to protect access ports using port security, TACACS/TACACS+, Radius, storm control, Access Control List both port, VLAN based.
8	Switch should have queuing as per IEEE 802.1P standard on all ports with mechanism for traffic shaping and rate limiting features for specified Host, network, Applications etc.
9	Should have Power supply 230 Volt 50Hz input
10	The switch should support IPv6 Guard, IPv6 RA-Guard, IPv6 DHCP- Guard, Source-Guard features
11	Switch should support automated image installation, configuration & automatic configuration of per port QoS to reduce switch provisioning time & effort.
12	Must have SNMP v1, v2, v3 from day one

Sr. No.	Specifications
13	Should have CLI and GUI based management console port.
14	The switch should support IEEE 802.3az from day-1
15	The switch should be IPv6 ready
16	The proposed switch should be EAL2/ NDPP certified by common Criteria body at the time of delivery.

WAN Router:

Sr. No.	Parameter	Specifications
1	Architecture	Router should have redundant controller cards and should support stateful switchover, non-stop forwarding, Non-stop routing and Graceful restart.
		Router should be CE2.0/MEF14.0 certified
		Router shall support MEF for Ethernet based services like PW, VPLS or ATOM.
		Router shall support sync any configurations from previous modules to new modules with hot-swap event occurred
		The router should have redundant control & data plane.
		The router shall support following type of interfaces – 10GE, 1GE interfaces, 10G, Ch.STM1
		All the Ports and card on Router should be hot swappable and field replacement of port or card should not require to bring down the chassis.
2	Performance	Router shall support non-blocking capacity of 64 Gbps full duplex
		Router shall support 60 Mpps forwarding performance for IPv4 & IPv6 performance
		The router should support 20Gbps per slot throughput.
		Router shall support 16000 Mac addresses
		Router shall support 18000 IPv4 routes
		router shall support 4000 queues and 128 MPLS VPN's
		Router shall support aggregation of links. Minimum 8 links should be supported as part of single aggregation

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

		Shall support Strict Priority Queuing or Low Latency Queuing to support real-time application like Voice and Video with minimum delay and jitter.
		Congestion Management: WRED, Priority queuing, Class-based weighted fair queuing
6	Security & Management	Support Access Control List to filter traffic based on Source & Destination IP Subnet,Source& Destination Port, Protocol Type (IP,UDP, TCP, ICMP etc.) and Port Range etc. Should Support per-user Authentication, Authorization, and Accounting through RADIUS or TACACS and SNMPv1/v2/V3
7	Operating Environmental Requirements	0ºC to 40ºC operating temperature and 10 to 90%, non-condensing
8	Interface	The proposed router should support the following from day1: - 2x10G SFP+ ports supplied with 1x10G single mode transceiver, 1x10G multi-mode transceiver, 8x1G SFP ports supplied with 4x1G single mode transceiver, 4x1G multi-mode transceiver & 32 no's of 10/100/1000 Base- T ports.
9	Certifications/ OEM	The proposed router should be EAL2/ NDPP certified or equivalentas per industry standards at the time of delivery. The router should be IPv6 ready from day-1.

Disaster Recovery (DR)

- The MSI is required to provision for a Disaster Recovery (DR) Site same as of main Data Center (DC) capacity & standard for Smart City Solution. The DR site should not be in the same seismic zone and should be at least 250 km from Main DC site.
- DR site shall provision to cater to 100% load of the smart city system.
- VSCL will avail hosting services from MEGHRAJ cloud. MSI will implement, manage the architecture accordingly.
- There shall be no loss of video recording in case of failure of any single server and storage component. Both DC and DR Site shall work in an Active-Active mode with 100% recording of cameras and application availability of all smart city components.

- The MSI shall establish dedicated connectivity between the DC and DR Site for replication & failover. The MSI shall submit the detailed solution document for the DR Site solution with justification for the proposed design meeting the requirements.
- Authority would carry out a detail assessment of the proposed location for the Smart City Data Center on the parameters of Safety & Security and reserves it right to accept or reject the proposed site for data center. In case the proposed site is not acceptable to Authority, Successful Bidder shall suggest alternatives matching the requirements mentioned above.
- Authority may also ask the respective bidder to arrange for a visit during bid evaluation stage.
- The MSI needs to offer the cost of the colocation, both for DC and DR site considering the requirement of Rack space, Seating space for the Technical/Project team and the electricity charges on yearly basis.

4.3 Smart Traffic & City Surveillance Management

For protecting the Citizens and ensuring public safety advanced ICT enabled security solutions are a pre-requisite to effectively fight threats from activities of terrorism, organized crime, vandalism, burglary, random acts of violence, and all other forms of crimes. CCTV based Video Surveillance is a one such security enabler and so it is envisaged to design, develop, implement and maintain a dedicated City Wide Video Surveillance System catering to the needs of the Varanasi Police it shall be housed.

Smart Traffic Management Overview

Competent Authority is the nodal agency for regulating and managing the entire road network and traffic signals in the Varanasi City. Currently, there are total 61following kinds of traffic junctions:

S No.	Arms	Number of Junctions
1	3	15
2	4	44
3	5	1
4	6	1
Total		**61**

Majorly, Varanasi City is having a large proportion of 4Arm traffic junction just like every other Indian City.

Currently, Varanasi City is lacking on advanced ICT enabled Traffic Management and Communication tools/systems and existing system.

The proposed technical solution should cater to the following challenges:

1. Traffic congestion and huge waiting time
2. No right of way to emergency vehicles like ambulance, police 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 Varanasi City traffic flow

Competent 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
8. Verification of vehicle related documents like Registration Certificate, Insurance Certificate, Pollution Certificate etc. by issuing a single E-Certificate/QRCode/Unique Code SMS.

Geographical Spread

Varanasi Police covers an area of about 112.26 Sq. km. The following map represents the Geographical spread of the area and zone wise distribution of police jurisdictions. This includes Varanasi Municipal Corporation limits.

***Varanasi* Municipal Corporation Map**

Solution Requirements:

The MSI shall be responsible for Supply, Installation, Implementation and Operation & Maintenance of Varanasi Surveillance System for a period of Five Years from the date of Go Live of the respective phase independently. The indicative requirement for MSI is broadly categorized into following:

#	Requirement	Indicative Scope of Work
1	**Min Surveillance**	1. Public Announcement System **(PAS)**
		2. **VMS** – Supply, Installation Poles and VMS, power, backup etc.

	System Infrastructure at field locations	3. Supply, Install Implement and Maintenance of IP based cameras with IR
		i. Dome +PTZ cameras
		ii. Fixed Box Camera
		Additional features with the camera
		Camera to support Adaptive Traffic Control System (ATCS)
		Camera to support ANPR
		Camera to support RLVD
		Camera with online FRS
		Cameras that support Analytics
		Sensor installation required for (ATCS)
		Note: There is no pole installation required for traffic signals. The cameras should be installed using appropriate fittings. Installation configuration and maintenance of Poles & required power, backup, network connectivity and any other additional hardware and software other fittings is in the scope of MSI
		Data Retention Period: 90 days
		Kindly refer Bill of Material for detailed location wise camera Distribution.
2	**Network Infrastructure**	1. Between camera & aggregation point – Field location
		2. Between aggregation points & Data center
		3. Between Data Center & KICCC
		4. Between Data Center & viewing/monitoring center
		5. It is envisaged that the MSI will coordinate ad take services of the existing Network Providers in Varanasi like BSNL, Reliance Jio, Airtel, Railtel, Vodafone, etc. However, a tri-partite Agreement among VSCL, MSI & the Network Service Providers would be signed in order to meet networking requirements as defined within Service Level Agreement.
3	**Data Center**	1. Supply & installation of all the requisite ICT Infrastructure including server, storage, network components and peripherals to handle 100% load along with provisioning for redundancy.
		2. Supply & installation of all the requisite Non IT infrastructure like furniture, AC, and interior work etc. excluding the civil work at the space, which will be provided by the Competent Authority.
4	**Integrated Command and Control Center**	1. Supply & installation of all the IT & Non IT infrastructure such as the Video Wall, Workstation, Furniture, AC, and interior work, etc. excluding civil work at the space provided by Competent Authority

	(KICCC)	2. The MSI should note that the KICCC would be working as a single source for monitoring all the Operational aspects of the Smart City Solutions and hence, the Supply & installation of ICT & Non ICT infrastructure like Video Wall, Workstation, Furniture, AC, and interior work etc. (excluding the civil work) at the space provided by the Competent Authority, is also to be carried out by the MSI.
		3. MSI should also consider to have Meeting and discussion rooms with required components that include furniture, phone, projector etc. but not limited to.
5	**Applications at KICCC**	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)
		6. Integration with existing criminal records of Varanasi
		7. Analyze and implement User specific requirement implementation
		8. ATCS Implementation
6	**Video Feeds other than KICCC**	MSI is expected to provision for viewing of feeds at selected key police locations is required
7	**Capacity Building**	MSI is to provide all Technical & Functional training/capacity building/handholding for the designated officials/staff/personnel on a continuous basis

Surveillance System Infrastructure at Field Locations

This Component covers planning & implementation of the Surveillance system comprising cameras and other field equipment at locations identified by Varanasi Competent Authority, Actual placement of pole & number of cameras at each location, type of cameras, fixation of height & angle for the cameras to ensure maximum coverage in consultation with Varanasi Competent Authority.

A detailed survey shall be conducted, by the MSI along with a team of Competent Authority and Varanasi police, at each of the strategic locations. This survey shall finalize the position of all field equipment's 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 MSI and submitted to Competent 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. MSI shall prepare the Detailed Report for field level requirements such as e.g. Cameras (types & numbers), Camera Mounting requirements, Power Requirements, Connectivity Requirements etc. for perusal of Competent Authority. Indicative list of the field level hardware to be provided by MSI is as follows:

1. Cameras (Fixed Box Cameras, PTZ Cameras, ANPR cameras, FRS camera 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.

Supply & Installation of Camera Infrastructure

Based on detailed field survey as mentioned above, MSI shall be required to supply, install and commission the surveillance and monitoring systems at the identified locations and thereafter undertake necessary work

towards its testing.MSI 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 MSI while installing / commissioning cameras are as follows:

1. Ensure that surveillance and monitoring objective is met while positioning the camera such that the required field of view is being captured as finalized in field survey

2. Ensure that camera is protected from the on field challenges of weather, physical damage and theft.

3. Make proper adjustments so as 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. Deployment of Collusion preventive barriers around the junction box & pole foundation in case it's installed in collision prone place.

6. Deployment of 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.

Installation of Poles/Cantilevers/Gantry if required

1. The MSI shall ensure that all installations are done as per satisfaction of the Competent Authority.

2. For installation of Variable Message System (VMS), CCTV Cameras, PTZ Cameras, Public Address System, etc. MSI shall provide appropriate poles & cantilevers and any supporting equipment.

3. MSI shall be required to supply, install, configure and integrate surveillance cameras at the identified locations and thereafter undertake necessary work towards their commissioning.

4. MSI shall ensure that the poles erected to mount cameras are good, both qualitatively and aesthetically

5. MSI shall use the industry leading practices while positioning and mounting the cameras and ensure that the pole / mast implementation is vibration resistant. Arrangements for bird scare spikes on top of camera shall be made to prevent birds from sitting on top of camera box.

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 MSI.

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 MSI so that there is clear line of sight.

9. MSI shall be responsible to undertake required structural analysis regarding the regulated load conditions and considering the respective wind load while installing the poles / cantilevers for cameras and Variable Messaging Sign boards

10. MSI shall provide structural calculations and drawings for the approval of Competent Authority. The design shall match with common design standards as applicable under the jurisdiction of Competent Authority/authorized entity.

11. MSI 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. MSI shall ensure that physical look of the installation area returns to neat & tidy conditions after installation of poles, cantilevers etc. The placement shall be designed keeping in mind the normal flow of vehicular traffic and pedestrian movement is not disturbed.

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. MSI shall carry out a study and identify locations to provide UPS backup, depending upon power situation across Varanasi City, to meet the camera and other field equipment's uptime requirements.

3. MSI shall install UPS at the identified intersections in secure, tamper-proof housing in corrosion resistant cabinets.

4. MSI shall ensure that the UPS is suitably protected against storms, power surges and lightning.

5. MSI shall provide UPS for efficient heat dissipation without air conditioning. It shall be able to withstand temperatures prevalent in Varanasi 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. MSIs 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 Varanasi's environmental conditions. They shall have separate lockable doors for:

    a) Power cabinet: This cabinet shall house the electricity 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, FRS, 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. MSI shall ensure that all the hardware is placed inside the junction boxes that could withstand temperatures prevalent in Varanasi throughout the year

Civil and Electrical Works

1. MSI shall be responsible for carrying out all the civil & Electrical 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

2. MSI shall provide city to the cameras through the aggregation point. Since this component has dependency on approval from local authorities, it is recommended that MSI plans this requirement well in advance & submits the application to the concerned electricity City distribution agency with requisite fees, as applicable

3. MSI shall carry out all the electrical work required for powering all the components of the system

4. Electrical installation and wiring shall conform to the electrical codes of India

5. MSI 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

6. For the wired Box cameras, MSI 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

7. Registration of electrical connections at all field sites shall be done in the name of the Competent Authority.

8. MSI shall house the electricity meters inside the power cabinet as mentioned in the controller Cabinet section as above.

Earthing and Lightning Proof Measures

1. MSI shall comply with all 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. MSI 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 (Complementary metal–oxide–semiconductor 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.

Public Address System (PAS)

Public Address System shall be used at intersections, public places, market places or those critical locations as identified by Competent Authority to make important announcements for the citizens/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 use PoE power that could drive the speakers. The system shall also contain the control software that could be used to control/monitor all the components of the system that includes Controller, Calling Station & keypad, Amplifier (Mixing & Booster).

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

Variable Message Signboards (VaMS)

Variable Message Signboard (VMS) shall be installed at identified strategic locations. The VMS 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 MSI 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 VMS unit shall be able to communicate with the Integrated Command and Control Centre System (ICC) using GSM Data/ Wi-Fi/ Ethernet/SMS Channel. GSM data channel (GPRS) / Wi-Fi 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 Integrated Command and Control Centre System (KICCC).

VMS shall be managed and operated from the Integrated Command and Control Centre (KICCC) system using handled by a server where information in the form of data messages shall be fed in a

manner to be displayed on a specific VMS installed at a particular location or across all locations. The VMS boards shall be viewable from a distance of 100m and various angles on the road.

For installing VMS Signboards, the MSI 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. MSI shall consider additional space for lateral clearance as well as a vertical clearance height as per NHAI (National Highway Authority of India) guidelines.

Variable messaging System will be used by other applications like ITMS, Smart Parking, Environment monitoring etc as mentioned in respective sections.

Pelican Signals:

Pelican Signal (Pedestrian Light Controlled Crossing) shall be a definitive light controlled crossing signal featuring a set of traffic lights (Green Man & Red Man Signal) with a push button, operated by pedestrian and shall also be able to facilitate differently-abled/Senior Citizens for crossing. The controls to operate the light signals shall be on the pedestrian's corner while the light signal for crossing on the other side of the road. Pelican Signal shall be installed at identified locations.

Configuration

Sample drawings below is for indicative purpose only; the bidders may propose their own design meeting the specifications of a Pelican Signal.

Figure : Indicative Representation of Pelican Signal.

Miscellaneous:

1. Competent Authority shall assist in obtaining all necessary go ahead, legal permissions, NOC (No Objection Certificate) from various departments to execute the project. MSI shall have to identify and obtain necessary legal / statutory clearances for erecting the poles and installing cameras, for provisioning of the required power, etc.MSI shall provide & manage all necessary paper work to pursue permission from respective authorities. No commercial/legal fees (except the RoW charges) shall be applicable to Competent Authority for obtaining the necessary permissions. These shall be provisioned by the MSI in their financial bid

2. The MSI shall provide all material required for mounting of components such as cameras, VMS 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, Hardware, Software and workmanship which form a part of the MSI services will be under O&M to be undertaken by the MSI throughout the contract period.

4. MSI shall also get comprehensive insurance from reputed insurance company for the project duration for all the equipment's/components installed under this project.

5. MSI 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 Competent 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 Competent Authority or its designated agency. A report has to be maintained and submitted to VSCL.

7. In addition to above, the MSI shall be fully responsible for all maintenance activities for the period between installation of equipment and roll-out of the system.

8. During implementation, if observed that any camera / field equipment requires change in the field of view / orientation, it shall be done by MSI without any extra cost.

9. In case of request for change in location of field equipment post installation, the same shall be borne by Competent Authority at either a unit rate as per commercials or a mutually agreed cost.

KPIs for Traffic Management

1. **Improve Journey Time**- Improve reliability in journey times between various locations, so that citizens can experience an enhanced quality of road based transportation, through improving sustainability and efficiency in operation of the road network.

2. **Increase Signal Efficiency**- Reduction in traffic delays, optimized cycle times at intersection to regulate and maintain free flow of traffic to enhance the efficiency of the transport infrastructure.

3. **Increase Operational Efficiency**- Varanasi Traffic Police intends to spend more time on the public facing functions. Thus Information technology solutions should help in reducing the repetitive paperwork/records and making the back-office functions more efficient.

4. **Improve Customer Services**- The traffic services to the public can be improved through the user friendly presentation of the various traffic information in real time through sharing of all relevant data feeds for public consumption.

5. Implement efficient planning, operations and decision making system for Varanasi for better livability.

6. Implement traffic enforcement mechanism for traffic violation, checking and monitoring shall reduce the traffic related offences of Red Light violations.

7. Create a platform for sharing traffic information across the city- Mechanism to broadcast information regarding traffic, parking spaces and other incidents to police and citizens that hamper the traffic movements.

8. Provide safety for pedestrians.

9. Connect police and citizens through social media like Facebook and twitter to promote quick methods of interactions by using existing presence of citizens.

10. Website for Traffic rules & regulations, road safety, emergency service, details on traffic police-public interface, Challan notice information, and road safety measures.

11. Integrate e-Challan system if already exists.

12. Mobile App for Ambulance drivers to inform police regarding to and fro movement of vehicle from origin to incident and to destined hospital.

13. Use existing signals in the ecosystem and add additional components for Intelligent Traffic Management system.

14. Should be able to configure based on Ambulance, Buses, cars etc.

15. Feasibility study should include following KPIs:

    - Volumes of vehicles moving in the road network
    - Vehicle type distribution
    - Directional distribution
    - Physical and visual characteristics of the area
    - Travel times, delays between different points of the network
    - Emission
    - Additional dependencies with respect to the available infrastructure and geometry at the junctions
    - Any other relevant data which the bidder anticipates will assist in establishing the benchmarks for the project
    - Study existing RTT (Round Trip Time) for existing arterial roads and se goals to reduce RTT at different time of the day

Representation of components of Intelligent Traffic Management System

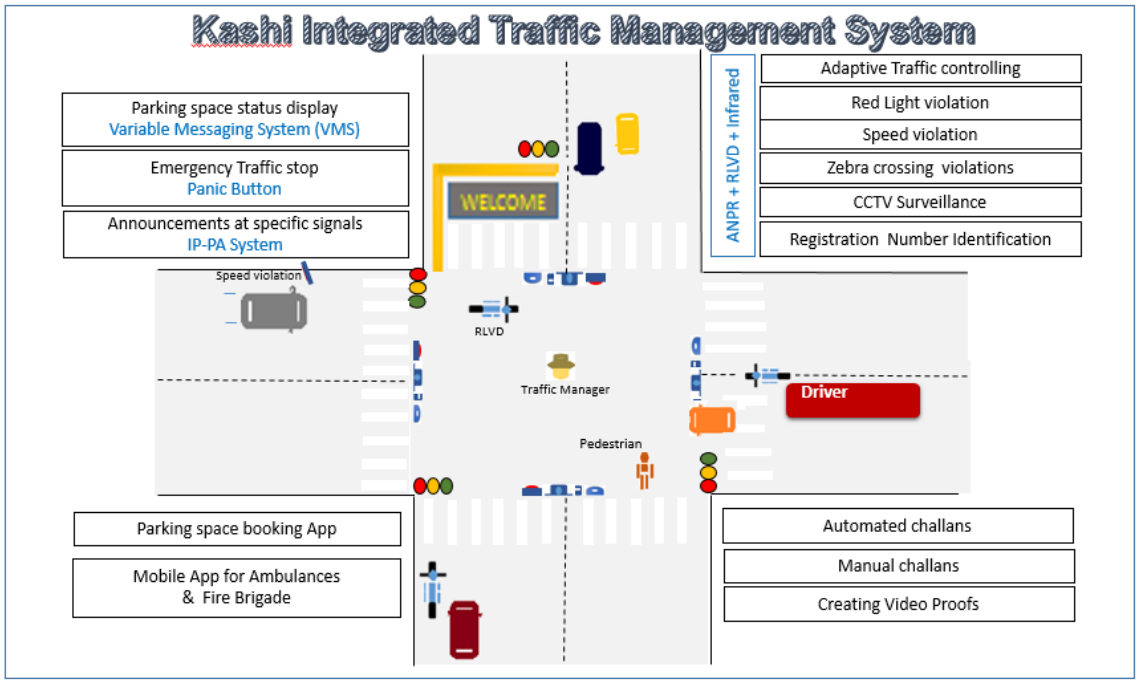


Figure : Illustrative Representation of Kashi Integrated Traffic Management System (ITMS).

Functional requirements of ITMS

Functional requirements of the Adaptive Traffic Control System (ATCS)

Adaptive Traffic Control System:

The Adaptive Traffic Control System has the following building blocks.

a. Traffic Signal Controller
b. Vehicle Detectors
c. Communication Network
d. ATCS Application Software
e. Traffic Management Centre

Traffic Signal Controller

The Traffic Signal Controller equipment is a 32 bit or 64-bit microcontroller with solid state traffic signal lamp switching module with the ability to program any combination of traffic signal stages, phases and junction groups. The controller will ideally have a conflict monitoring facility to ensure

that conflicting, dangerous are pre-flagged at the programming stage and these are disallowed even during manual override phase.

The Traffic Signal Controller will be adaptive so that it can be controlled through the central traffic control center as an individual junction or as part of group of traffic junctions along a corridor or a region. The signal controller design must be flexible for the junction could be easily configured to be part of any corridor or group definition and could be changed through central command controller easily.

Site specific configuration data shall be stored in a non-volatile memory device (FLASH memory) easily programmable at the site through keypad or laptop. A minimum of 512KB flash memory and 128KB RAM shall be provided. Volatile memory shall not be used for storing the junction specific plans or signal timings.

All timings generated within a traffic signal controller shall be digitally derived from a crystal clock which shall be accurate to plus or minus 100 milliseconds.

The controller shall provide a real time clock (RTC) with battery backup that set and update the time, date and day of the week from the GPS. The RTC shall have minimum of 10 years battery backup with maximum time tolerance of 10 sec per day.

The controller shall have the facility to update the RTC time from ATCS server, GPS and through manual entry.
The controller shall be capable of communicating with the ATCS server through Ethernet on a managed leased line network or any other appropriate stable communication network.

Police Panel

The controller shall provide the following facilities in a separate panel with provision for lock and key arrangements for use by the Traffic Police.

- Four Hurry Call switches: The Hurry Call mode will provide the means to force the controller to a defined stage, without violating safety clearances. A pre-emption input may be used to demand the Hurry Call mode to give right of way to emergency vehicles. It should be possible to configure the Hurry Call switches to any stage as per site requirements.
- One Forced Flash Switch: Activation of this switch should force the signal to Flashing Amber / Flashing Red.

- One Auto / Manual Switch: Activation of this switch should enable manual operation of the controller. Deactivation of the manual switch shall continue from the current stage without interruption.
- One Manual Advance Pushbutton Switch: In manual operation mode, the stages appear in the sequence specified in the signal plan timetable. Activating the pushbutton switch shall terminate the currently running stage and start the next, without violating safety clearances.
- One Junction OFF Switch: Activating this switch should put OFF all signal lamps. On deactivation of the switch the traffic signal controller shall resume its normal operation without violating any safety clearances.

Modes of Operation

The traffic signal controller shall have the following modes of operation:

- **Fixed Time:** In fixed time (pre-timed) mode the traffic signal controller shall execute stage timings according to the site specific timetable maintained in the traffic signal controller FLASH memory. Inputs from vehicle detectors shall be ignored in this mode and no pre-emption shall be made on any stage. Cycle time remains constant in every cycle execution for a given time period.
- **Vehicle Actuation with All Stages Pre-emption:** In the vehicle actuation with all stages pre-emption mode, the traffic signal controller shall execute stage timings as per demand from vehicle detectors within the constraints of Minimum Green, Maximum Green running period for the stage and Cycle time stored in the traffic signal controller FLASH memory. Pre-emption shall be possible for all demand actuated stages. Cycle time may vary in every cycle execution.
- **Semi-Actuation:** In the semi-actuation mode, the traffic signal controller shall execute stage timings in the vehicle actuated stages as per demand from vehicle detectors within the constraints of Minimum Green, Maximum Green running period for the stage and Cycle time stored in the traffic signal controller FLASH memory. All other stages shall execute the Maximum green time configured for the stage. Pre-emption shall be possible for all demand actuated stages. Cycle time may vary in every cycle execution.
- **Stage Skipping:** The traffic signal controller shall not execute the stage enabled for skipping when there is no vehicle demand registered for the stage till clearance amber time of the previous stage.
- **Vehicle Actuation with Fixed Cycle length:** In vehicle actuation with fixed cycle length mode, the traffic signal controller shall execute stage timings as per demand from vehicle detectors within the constraints of Minimum Green, Maximum Green running period for

the stage and Cycle time shall be maintained constant during a given timeslot. Pre-emption to be carried out for all demand actuated stages except for Priority Stage.

- **Full ATCS (FATCS):** In FATCS mode, the traffic signal controller shall execute stage timings as per demand within the constraints of Minimum Green, Maximum Green running period for the stage and Cycle time specified by the Central Computer during every cycle switching. Pre-emption for all demand actuated stages except Priority Stage shall be possible in this mode. The traffic signal controller shall identify a communication failure with the central computer within a specified time period. In such an event the signal plan timings shall be executed from the local timetable stored in the traffic signal controller FLASH memory. Fall-back mode of the traffic signal controller shall be vehicle actuated. On restoration of the communication with central computer the traffic signal controller shall automatically resort to FATCS mode.

The traffic signal controller shall accept commands for remote selection / de-selection of the following from the Central Computer at VMC.

- Hurry Call
- Flashing Amber / Flashing Red
- Junction Off

If not reverted to the normal operation within the time period listed below, the traffic signal controllers shall timeout the commands and operate normally

- Hurry Call – 5 Minutes
- Flashing Amber / Flashing Red – 30 Minutes
- Junction Off – 30 Minutes

The traffic signal controller shall report the following to the Central Computer through the communication network every cycle or on an event as appropriate.
Green time actually exercised for each approach (stage pre-emption timing) against the Green running period set for the approach by the Central Computer

Mode of Operation

- Lamp failure, if any
- Output short circuit, if any
- Detector failure, if any

Traffic Signal Controller Operating Parameters

Phases - The controller shall have facility to configure 32 Phases either for vehicular movement, filter green, indicative green, pedestrian movement or a combination thereof.

- It shall be possible to operate the filter green (turning right signal) along with a vehicular phase. The filter green signal shall flash for a time period equal to the clearance amber period at timeout when operated with a vehicular phase.
- The pedestrian phase signal shall be configured for flashing red or flashing green aspect during pedestrian clearance.
- It shall be possible to configure any phase to the given lamp numbers at the site.

Stages – The controller shall have facility to configure 32 Stages.

- Cycle Plans – The controller shall have facility to configure 24 Cycle Plans and the Amber Flashing / Red Flashing plan. It shall be possible to define different stage switching sequences in different cycle plans. The controller shall have the capability for a minimum of 32 cycle-switching per day in fixed mode of operation.
- Day Plans – The controller shall have facility to configure each day of the week with different day plans. It shall also be possible to set any of the day plans to any day of the week. The controller shall have the capability to configure 20 day plans.
- Special Day Plans – The controller shall have facility to configure a minimum of 20 days as special days in a calendar year
- Starting Amber – During power up the controller shall initially execute the Flashing Amber / Flashing Red plan for a time period of 3 Seconds to 10 Seconds. The default value of this Starting Amber is 5 Seconds. Facility shall be available to configure the time period of Starting Amber within the given limits at the site.
- Inter-green – Normally the inter-green period formed by the clearance Amber and Red extension period will be common for all stages. However, the controller shall have a facility to program individual inter-green period from 3 Seconds to 10 Seconds.
- Minimum Green – The controller shall allow programming the Minimum Green period from 5 Seconds to 10 Seconds without violating the safety clearances.

  It should not be possible to pre-empt the Minimum Green once the stage start commencing execution.
- All Red – Immediately after the Starting Amber all the approaches should be given red signal for a few seconds before allowing any right of way, as a safety measure. The controller shall have programmability of 3 Seconds to 10 Seconds for All Red signal.

- Signal lamps monitoring – The controller shall have inbuilt circuitry to monitor the lamp status.
- Green – Green Conflict Monitoring – The controller shall have a facility to list all conflicting phases at an intersection. The controller should not allow programming of these conflicting phases in a Stage. A hardware failure leading to a conflict condition (due to faulty devices or short circuit in the output) shall force the signal into Flashing Amber/ Flashing Red.
- Cable less Synchronization – It shall be possible to synchronize the traffic signal controllers installed in a corridor in the following modes of operation, without physically linking them and without communication network. GPS enabled RTC shall be the reference for the cable less synchronization.
- Fixed Time mode with fixed offsets.
- Vehicle Actuated mode with fixed offsets.

Input and Output facilities

- Lamp Switching: The controller shall have minimum 64 individual output for signal lamp switching, configurable from 16 to 32 lamp groups where in each group is RED, AMBER & GREEN. The signal lamps may be operating on appropriate DC/AC voltage of applicable rating.
- Detector Interface: A minimum of 16 vehicle detector inputs shall be available in the controller. All detector inputs shall be optically isolated and provided with LED indication for detection of vehicle.
- Communication Interface: The traffic signal controller shall support Ethernet interface to communicate with the ATCS server.
- Power Saving: Bidders are requested to propose appropriate energy saving mechanisms and approaches. The traffic signal controller shall have a facility to regulate the intensity of signal lamps during different ambient light conditions.
- Real-time Clock (RTC): The GPS receiver for updating time, date and day of the week information of the traffic signal controller should be an integral part of the traffic signal controller.
    - The traffic signal controller shall update the date, time and day of the week automatically from GPS during power ON and at scheduled intervals.
    - Manual entry for date, time and day of week shall be provisioned for setting the traffic signal controller RTC (Real Time Clock).
    - It shall be possible to set the RTC from the Central Server when networked.

- Keypad (optional): The traffic signal controller shall have a custom made keypad or should have provision for plan upload and download using PC/laptop/Central Server.
- Operator Display (optional): The traffic signal controller shall optionally have a LED backlit Liquid Crystal Display (LCD) as the operator interface.

Vehicle Detector:

- The bidder shall propose appropriate technical solution / product to count vehicles at each arm of the traffic junctions. The outputs of the detectors shall indicate the presence of vehicles and shall be used to influence the operation of the traffic signal controller and shall generate counts, demands and extensions for right-of-way. Means shall be provided so that a detector may be connected to demand and / or extend a phase movement as specified.
- The contractor shall clearly specify the placement of the detector (upstream, downstream, stop line, exit etc.) for independent straight and right turn signals.
- The detector shall be able to count vehicles in non-lane based mixed traffic flow conditions and differentiate between different vehicle types (two-wheeler, three-wheeler, car, HGV, etc.). The accuracy of counts shall be bigger than 90% over all light and weather conditions. The contractor shall clearly specify in their technical proposal how this will be accomplished.
- The contractor shall give an estimate of the total number of vehicle presence detection zones and vehicle detectors required and the type of detection system recommended.
- A detector that does not change its status at least once during a stage execution shall be notified to the Central Computer (in ATCS mode) at the termination of the associated stage.

Communication Network

Function of the Communication network is for remote monitoring of the intersection and its management. Real time data (like RTC time, stage timing, mode, events, etc.) from the traffic signal controller is required to be sent to the Central Computer in Traffic Management Centre. Central Computer running the ATCS application shall calculate and send optimum signal timings to all intersections in the corridor. The contractor shall clearly specify the bandwidth requirements and the type of network recommended for the ATCS. The contractor shall specify the networking hardware requirements at the Traffic Management Centre and remote intersections for establishing the communication network.

ATCS Application software

Objective of the ATCS is to minimize the stops and delays in a road network to decrease the travel time with the help of state-of-the-art technology. The adaptive traffic control system will provide simulation based real time traffic flow modelling capability with the capacity to calculate traffic flows, OD movements, and queues and turning movement along entire primary road transport network in the defined study area covering the ATCS junctions and beyond. The Application software or platform will be able to predict traffic flow in the network for the near term over various interval horizons (e.g. T+5, T+10 … T+30 mins). The ATCS application will provide estimated traffic flow for each of the junction to calculate optimal cycle times, effective green time ratios, and change intervals for all system traffic signal controllers connected to it either as individual junctions or groups of junctions. These calculations will be based up on assessments carried out by the ATCS application software running on a Central Computer based on the data and information gathered by vehicle detectors at strategic locations at the intersections controlled by the system. The ATCS application software shall be divided into two module with the following are the expected capabilities of the individual modules:

Module 1: Real Time Traffic Prediction Capability

- Shall provide a decision support tool for assessing strategies to minimize congestion, delays and emergency response time to events via simulation and planning tools liked with real time traffic data fusion and control of traffic signaling infrastructure on ground.
- Shall collect continuously information about current observed traffic conditions from a variety of data sources (like Bus GPS data, parking data, mobile phone data etc. Bidders can propose alternate data sources that could be integrated) and of different kind (traffic states, signal states, vehicle trajectories, incidents, road works etc.)
- Shall infer a coherent and comprehensive observed traffic state (speeds, vehicular densities, and presence of queues) on all network elements, from above mentioned observations, including vehicle trajectories, through a number of map matching, data validation, harmonization and fusion processes.
- Shall have a Graphical User Interface (GUI) to be able to display traffic state along the observed and unobserved parts of the network through GIS maps (Varanasi is in process of implementing an enterprise GIS System). The bidder is expected to create a layer of edge equipment within that GIS platform and integrate with ATCS modules of the transport network and must be able to display traffic flow, building of queues, delays, location of traffic signals and junctions, key Points of Interests (POI), Variable Message signs etc. In addition, the GUI must be:

- Flexible for the operators to zoom and navigate with ability to interact with objects on the map.
- Should be interoperable across multiple platforms and key graphical results and MIS must be made available across the Web
- Graphically present time-space diagram for selected corridors on desktop
- Graphically present signal plan execution and traffic flow at the intersection on desktop

- Shall have the ability to predict, forecast and estimate the traffic pattern across the signals over the near term future (e.g. T+5, T+10, T+15, T+30 mins … T + 1 hour)
- Shall extrapolate the measurements made on a limited number of junctions and arms along the rest of the unmonitored network, and obtain an estimation of the traffic state of the complete network and the evolution of this traffic state over the near term future (e.g. T+5, T+10, T+15, T+30 mins … T + 1 hour)
- Shall be able to forecast the traffic state with respect to current incidents and traffic management strategies (e.g. traffic signal control or variable message signs), improving the decision making capabilities of the operators even before problems occur
- Shall provide customizable estimates of Key Performance Indicators (KPI) for alternate traffic management strategies to quickly assess the results
- Shall provide calculated traffic flows estimation and forecast, queues and delays to Urban Control and Adaptive Traffic Control Systems, allowing for proactive Traffic Management and Control.
- To raise alerts to the operator that trigger on customizable conditions in the network (starting with simple drops in flow, up to total queue lengths along emission sensitive roads surpassing a definable threshold); To distribute both collected and calculated traffic information via a variety of communication protocols and channels, ensuring high interoperability degree and thus acting as a "traffic data and information hub.
- Shall include a traffic data warehouse (for minimum 5 years) for all historic traffic information gathered from the hardware installed on the road network. Bidder to propose how data storage requirements could be minimized using consolidation techniques.
- Shall operate in real time that is continuously updating the estimates on the state of the network and the travel times on the basis of data collected continuously over time.
- Shall operate the traffic lights with the adaptive traffic controls, based on the current and

- Forecasted traffic demand and the current incidents, thus optimizing the green waves continuously throughout the network
- Shall be possible to interface the ATCS with a popular microscopic traffic flow simulation software for pre and post implementation analysis and study of the proposed ATCS control strategy.

Module 2: Adaptive Traffic Control System

- To operate the traffic lights with the adaptive traffic controls, based on the current and forecasted traffic demand from the above Real Time Traffic Prediction Tool including the current incidents, thus optimizing the green waves continuously throughout the network.
- Enable a smart public transport priority respecting the delays for all road users at once with the adaptive signal controller. To have the capability to integrate with Bus GPS data to identify oncoming buses at the junction and be able to provide priority clearance of buses.
- Identify the critical junction (Master Junction) for each of the defined corridor or a region based on maximum traffic demand and saturation.
- The critical junction cycle time estimated shall be used as the group cycle time i.e. cycle time common to all intersection in that corridor or region.
- Stage optimization to the best level of service shall be carried out based on the traffic demand.
- Cycle optimization shall be carried out by increasing or decreasing the common corridor cycle time based on the traffic demand within the constraints of Minimum and Maximum designed value of cycle time.
- Offset correction shall be carried out to minimize number of stops and delays along the corridor for the priority route and for the adjoining road network at once. Offset deviation shall be calculated with a traffic flow model based on the distance, traffic demand and speed between successive intersections and be corrected within 5 Minutes maximum.
- The system shall have provision to configure priority for upstream signals as default. The ATCS software shall continuously check the traffic demand for upstream and downstream traffic and automatically assign the priority route to the higher demand direction.

- The system shall use optimization algorithms that minimize a function based on the delays, number of stops and queue lengths simultaneously, using a traffic flow model, thus providing a true optimum for all road users.
- Develop appropriate stage timing plans for each approach of every intersection under the ATCS, based on real time demand and the predicted traffic flow values from the traffic flow model.
- Propose timing plans to every intersection under the ATCS at least every five minutes.
- Calculate the current queue lengths for each approach that has detection cycle-by-cycle based on the succession of time gaps between cars.
- Adjust the proposed timing plans second-by-second according to the current and past detector states and the current queue lengths for every intersection under detection.
- Enable transit signal priority with minimal disruption of car traffic, dependent on predefined weights for public transport vehicles in comparison to individual traffic. In order to decrease the workload for operation and maintenance, each supply item (road network, lanes, signals and detectors) shall be supplied just once, so that the all macro and microscopic traffic models and the microscopic traffic flow software used for calibration and verification of the ATCS share the same supply.
- Shall provide calculated traffic flows estimation and forecast, queues and delays to Urban Control and Adaptive Signal Control Systems, allowing for proactive Traffic Management and Control. Such estimation will be updated at least every 5 minutes or less, and will not be based on a machine learning approach that would not provide enough flexibility in case of unexpected events.
- Should be able to route emergency vehicles to minimize the impact of events on the travel time of emergency vehicles.
- Shall be able to export the calculated traffic flow data continually to a multi-modal journey-planner that allows all internet users in the city to find the best route with each traffic mode based on the current travel times in the network.
- Identify Priority routes and synchronize traffic in the Priority routes.
- Manage and maintain communication with traffic signal controllers under ATCS.
- Maintain database for time plan execution and system performance.
- Maintain error logs and system logs.
- Generate Reports on request.
- The ATCS shall generate standard and custom reports for planning and analysis.

Reports

System shall generate Corridor based and Intersection based reports. The application software shall generate the following reports, but not limited to the below. All the reports shall be possible for selected dates.

- Intersection based reports
- Stage Timing report – The report shall give details of time at which every stage change has taken place. The report shall show the stage sequence, stage timings and stage saturation of all stages of all cycles for a day. The saturation is defined as the ratio between the available stage timings to the actual stage timing executed by the traffic signal controller for the stage (stage pre-emption time).
- Cycle Timing report – The report shall give details of time at which every cycle has taken place. The report shall show the cycle sequence and cycle timings for all the cycles in a day.
- Stage switching report – The report shall give details of time at which a stage switching has taken place. The report shall show the stage sequence, stage timings and stage saturation for a day.
- Cycle Time switching report – The report shall give details of time at which a cycle switching has taken place. The report shall show the cycle sequence and cycle timings for the cycle in a day.
- Mode switching report – The report shall give details of the mode switching taken place on a day.
- Event Report - The report shall show events generated by the controller with date and time of event.
- Power on & down: The report shall show time when the master is switched on, and last working time of the master controller.
- Intensity Change – The report shall show the brightness of the signal lamp is changed according to the light intensity either manually through keypad or automatically by LDR with time stamp.
- Plan Change – The report shall show the time of change of plan either through keypad or remotely through a PC or Server.
- RTC Failure – The report shall show the time when RTC battery level goes below the threshold value.
- Time Update – The report shall show the time when the Master controller updated its time either manually through keypad, automatically by GPS or through remote server.

- Mode Change – The report shall show the time when Master controller's operating mode is changed either manually through keypad or a remote server. The typical modes are FIXED, FULL VA SPLIT, FULL VA CYCLE, FLASH, LAMP OFF and HURRY CALL.
- Lamp Status Report – The report shall show lamp failure report with date and time of failure, color of the lamp and associated phase.
- Loop Failure Report – The report shall show the date and time of detector failure with detector number and associated phase.
- Conflict – The report shall show the conflict between lamps (RED, AMBER, GREEN) in the same phase or conflict between lamps with other phase.
- Corridor Performance Report – The report shall show the saturation of all the intersections in a corridor for every cycle executed for the corridor and the average corridor saturation for a day.
- Corridor Cycle Time Report – The report shall show the Corridor cycle time, Intersection cycle time, Mode of operation and degree of saturation of all the intersections in a corridor for every cycle for a day

Graphical User Interface

The application software shall have the following Graphical User Interface (GUI) for user friendliness, which will have the following functionalities in additions to those described above.

- User login – Operator authentication shall be verified at this screen with login name and password
- Network Status Display – This online display shall indicate with appropriate color coding on site map whether an intersection under the ATCS is online or off. On double clicking the intersection a link shall be activated for the traffic flow display for the intersection.
- Traffic Flow Display – This online display shall indicate the current traffic flow with animated arrows, mode of operation, stage number being executed and elapsed stage time.
- Saturation Snapshot – This display shall show the current saturation levels of all intersections in a corridor.
- Reports Printing / Viewing – This link shall allow selection, viewing and printing of different reports available under ATCS
- Time-Space Diagram – The time-space diagram shall display the current stages being executed at every intersection in a corridor with immediate previous history.
- Junctions shall be plotted proportional to their distance on Y-axis and time elapsed for the stage in seconds on X-axis.

- Junction names shall be identified with each plot.
- Facility shall be available to plot the time-space diagram from history
- Currently running stage and completed stages shall be identified with different colors.
- Stages identified for synchronization shall be shown in a different color.
- Speed lines shall be plotter for stages identified for synchronization to the nearest intersection in both directions.
- It should be possible to freeze and resume online plotting of Time-Space diagram.
- The system shall have other graphical interfaces for configuring the ATCS, as appropriate

Functional Requirements of the Red Light Violation Detection Systems (RLVD)

Sr. No.		System Parameter
1		**General**
	a	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
	b	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.
	c	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
	d	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

Sr. No.		System Parameter
		should be clearly identifiable and demarcated in the image produced by the camera system.
	e	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 color of the Traffic light at the instant of Infraction even if any other means is being used to report the color of the light.
	f	The system should interface with the traffic controller to validate the color of the traffic signal reported at the time of Infraction so as to give correct inputs of the signal cycle.
	g	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 VMC. The network should have the capability to provide the real time feed of the evidence camera to the VMC at the best resolution possible on the available network
	h	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.
	i	In case of violation, lights should flash immediately
2		**Recording & display information archive medium**
	a	The recording and display of information should be detailed on the snapshot of the infracting vehicle as follows:
	b	Computer generated unique ID of each violation
	c	Date (DD/MM/YYYY)
	d	Time (HH:MM:SS)
	e	Equipment ID
	f	Location ID
	g	Carriageway or direction of violating vehicle
	h	Type of Violation (Signal/Stop Line)
	i	Lane Number of violating vehicle
	j	Time into Red/Green/Amber
	k	Registration Number of violating vehicle
	l	The size of file chunks that a camera should send to CC should be configurable
3		**On site-out station processing unit communication & Electrical Interface**

Sr. No.		System Parameter
	a	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.
	b	The system should have secure access mechanism for validation of authorized personnel.
	c	Deletion or addition and transfer of data should only be permitted to authorized users.
	d	A log of all user activities should be maintained in the system.
	e	Roles and Rights of users should be defined in the system as per the requirements of the client
	f	All formats of the stored data with respect to the infractions should be Non Proprietary
	g	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.
	h	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
	i	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.
4		**Mounting structure**
	a	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. MSI shall be responsible to carry out the site survey to assess site requirement including pole height/suitable structure for installation at various places in the city.
	b	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.

Sr. No.		System Parameter
	c	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.
	d	Rugged locking mechanism should be provided for the onsite enclosures and cabinets.
5		**RLVD Application**
	a	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 application should allow for viewing, sorting, transfer & printing of violation data.
	b	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.
	c	All outstation units should be configurable using the software at the Central Location
	d	Violation retrieval could be sorted by date, time, location and vehicle registration number and the data structure should be compatible with Varanasi Police database structure. It should also be possible to carry out recursive search and wild card search
	e	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).
	f	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.
	g	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 MSI.
	h	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

Sr. No.		System Parameter
		in such cases the printing should be possible along with the magnified image
	i	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.
	j	Apart from role based access, the system should also be able to define access based on location.
	k	Rights to different modules / Sub-Modules / Functionalities should be role based and proper log report should be maintained by the system for such access.
	l	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
	m	The evidence of Infraction should be encrypted and protected so that any tampering can be detected.
	n	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.
	o	System shall use open standards and protocols to the extent possible and declare the proprietary software wherever used.
	p	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.
	q	The data provided for authentication of violations should be in an easy to use format as per the requirements of user
	r	User should be provided with means of listing the invalid violations along with the reason(s) of invalidation without deleting the record(s).
	s	Basic image manipulation tools (zoom etc.) should be provided for the displayed image but the actual recorded image should never change.
	t	Log of user actions be maintained in read only mode. User should be provided with the password and ID to access the system along with user type (admin, user).
	u	Image should have a header/footer depicting the information about the site IP and violation details like date, time, equipment ID, location ID, Unique ID of each violation, lane number, Regn. Number of violating vehicle and actual violation of

Sr. No.		System Parameter
		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.
	v	Number plate should be readable automatically by the software/interface. There should be user interface for simultaneous manual authentication / correction and saving as well. Number plate should be readable automatically by the software/interface. There should be user interface for simultaneous manual authentication / correction and saving as well
	w	Interface for taking prints of the violations (including image and above details).

Functional Requirements of the Variable Message Sign Boards: (VaMS)

Sr.No.		Description
1		**System Requirements**
	a	The system should be capable to display warnings, traffic advice, route guidance, emergency messages and any other dynamic, customized messages from the VMC in real time.
	b	The system should also be capable to display warnings, traffic advice, route guidance and emergency messages to motorist by using local PC/Laptops.
	c	The VMS should display text (multi lingual – Marathi, Hindi & English) and graphic messages using Light Emitting Diode (LED) arrays.
	d	The System should able to display failure status of any LED at KICCC.
	e	The System should support Display characters in true type fonts and adjustable based on the Operating system requirement
	g	The VMS workstation at the KICCC should communicate with the VMS controller through the network. It should send out command data to the variable message sign controller and to confirm normal operation of the signboard. In return, the VMS workstation should receive status data from the VMS controller.
	g	VMS controllers should continuously monitor the operation of the VMS via the provided communication network.
	h	Operating status of the variable message sign should be checked periodically from the KICCC.

Sr.No.		Description
	I	It shall be capable of setting an individual VMS or group of VMS's to display either one of the pre-set messages or symbols entered into the computer via the control computer keyboard or by another means.
	J	It shall be capable of being programmed to display an individual message to a VMS or a group of VMS's at a pre-set date and time.
	k	A sequence of a minimum of 10 messages/pictures/ pre-decided sign or group of signs shall be possible to assign for individual VMS or group of VMS's.
	l	It shall also store information about the time log of message displayed on each VMS. The information stored shall contain the identification number of the VMS, content of the message, date and time at which displayed message/picture starts and ends.
	m	The central control computer shall perform regular tests (pre-set basis) for each individual VMS. Data communication shall be provided with sufficient security check to avoid unauthorized access
2		**Variable Message Sign board application**
	a	Central Control Software allows controlling multiple VMS (up to 10) from one console.
	b	Capable of programming to display all types of Message/ advertisement having alphanumeric character in English, Hindi, Marathi and combination of text with pictograms signs.
	c	Capable of controlling and displaying messages on VMS boards as individual/ group.
	d	Capable of controlling and displaying multiple font types with flexible size and picture sizes suitable as per the size of the VMS.
	e	Capable of controlling brightness & contrast through software.
	f	Capable to continuously monitor the operation of the Variable Message sign board, implemented control commands and communicate information to the Traffic Monitoring Centre via communication network.
	g	Real time log facility – log file documenting the actual sequence of display to be available at central control system
	h	Multilevel event log with time & date stamp
	i	Access to system only after the authentication and acceptance of authentication based on hardware dongle with its log.
	j	Location of each VMS will be plotted on GIS Map with their functioning status

Sr.No.		Description
		which can be automatically updated.
	k	Report generation facility for individual/group/all VMSs with date and time which includes summary of messages, dynamic changes, fault/repair report and system accessed logs, link breakage logs, down time reports or any other customized report.
	l	Configurable scheduler on date/day of week basis for transmitting pre-programmed message to any VMS unit
	m	Various users should 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.
	n	Apart from role based access, the system should also be able to define access based on location
	o	Rights to different modules / Sub-Modules / Functionalities should be role based and proper log report should be maintained by the system for such access
	p	Components of the architecture must provide redundancy and ensure that there are no single points of failure in the key project components. To take care of remote failure, the systems need to be configured to mask and recover with minimum outage.
	q	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.
	r	System shall use open standards and protocols to the extent possible
	s	Facility to export reports to excel and PDF formats.
3		**Remote Monitoring**
	a	All VMS shall be connected/configured to Traffic Monitoring Centre for remote monitoring through network for two way communication between VMS and control Room to check system failure, power failure & link breakage.
	b	Remote Diagnostics to allow identifying reason of failure up to the level of failed individual LED.

e-Challan system application:

The objective of the e-Challan application is as follows:

1. Issuing challan for traffic violations on a 24x7 basis.
2. Maintaining the details pertaining to all the activities of the Traffic circles/violations/violators.

3. Providing requisite structured/unstructured information to the traffic management officials as and when required.
4. Generating various statutory reports for the administrative use and functioning of the Traffic unit in matters of prosecution of violators and monitoring the functioning of field officers.
5. Integrating and networking the system with state-of-the-art hardware and application software for the Traffic Police to access and using the information in their day-to-day work.

Functional Requirement of the Vehicle Verification System (Subset of Smart Kashi Mobile App and Smart Kashi Portal):

1. Module shall have feature for uploading of vehicle related documents like Vehicle Registration Certificate, Insurance Certificate, Pollution Control Certificate etc. and related details.
2. Details of these documents will be accessed by Dept. of Police for verification.
3. On successful Verification of all documents Dept. of Police will issue an E-Certificate to the citizen in the form of QR Code/Unique Code SMS/PDF. Validity of E-Certificate shall be based on the validity of documents submitted.
4. On expiry of e-certificate citizen will have to upload the renewed copy of the expired document on the portal and a new E-certificate will be issued after verification.
5. Module shall have the facility to alert the citizen before expiry of the certificate in the form of alert sms, app notification etc.
6. Module shall also have the feature to manually add and upload details of documents through designated authorities on behalf of the citizen.
7. Integration with e-challan system for quick and hassle free verification of documents.
8. MSI shall integrate this module with Govt. of India Vehicle information portals like Vaahan, Saarthi, Insurance Companies etc. for verification.

Functional requirements of the e-Challan System:

1. e-challan software shall work in client -server mode, where the handheld devices units, workstation units will act as clients connected to the server through cellular network for data transfer.
2. e-challan system shall be able to retrieve vehicle owners details and vehicle data from RTO data base to minimize data entry.
3. e-challan system shall be able to retrieve vehicle registration details and driving license details by reading appropriate smart card to minimize data entry.
4. Server should maintain log of all current devices. Any access to the system must be recorded along with date, time, user id and IP address

5. Traffic officer should log in to the hand held device through the unique user id and pass word or smart card issued for the purpose
6. A unique Challan number should be generated through client software for each challan
7. As soon as a vehicle registration number is entered, the handheld device should automatically check from the server if the vehicle is stolen, wanted in any criminal case or is in the list of suspicious vehicle
8. The most frequent traffic offences should be kept at the top in the drop down menu and offence ingredients should be available if required by officer
9. Date, time and GPS coordinates of place of challan should be automatically populated in the relevant fields of client software
10. Compounding amount must populate in the field automatically from master table
11. The successful bidder should develop the GUI and functionality as per requirements of the Varanasi Traffic Police
12. The GUI should be Multi lingual i.e. English, Hindi and any other local language.
13. It should be possible to integrate payment gate way operator with the system for facilitation of payment
14. The Application Software should work in a web based environment.
15. The application software should be user friendly, easy to operate
16. The software must provide comprehensive data back-up and restoration capability.
17. The system will function in web-based system where the hand-held device shall work as a node
18. The application software should maintain the logs of user activities to facilitate the audit trail.
19. The system should have sufficient security features such as firewall, access control system, biometrics, password protection, audit trail, anti-virus etc.
20. Database server should be able to handle the activities of all the handheld devices at one time simultaneously with huge database size of prosecution, ownerships, driving license etc. without affecting the performance.
21. The software should be able to generate various periodical reports, summaries, MIS reports, query reply etc. as per the requirements of Varanasi Traffic Police.
22. Administrator should be able to modify the master tables as and when required and should have the capability to push the changes to hand-held devices.
23. All database tables, records etc. required for various dropdown menus etc. shall also be created by the vendor.
24. The application software is to be provided by the vendor to handle various processes of the prosecution required by the office of senior police officers, Courts etc.

25. Smart Certificate Module - document verification for citizen like Registration Certificate, Insurance Certificate, Pollution Certificate etc. and issuing a single renewable E-Certificate so that the citizen won't have to carry all documents.
26. Smart certificate will enable citizen with hassle free verification process making citizen worry free of carrying multiple documents. A unique code to be generated with E-Certificate to verify the vehicle owner details.

Hand Held Devices for e-Challan system

1. The Hand held device should be light weight and easy to hold.
2. Once the application is loaded on the hand-held device there should be no possibilities to modify the application by the user. Reloading and modifying of application should be possible only by an administrator.
3. On switching on the hand-held device the system must give access only after validation through user ID and password.
4. The communication between the server and hand-held device would be through GSM/GPRS/ 3G or better connectivity etc.
5. Every challan created must have a unique self-populated number.
6. The HH application must be able to access information from the main Server and display upon request, pop- up tables/codes, vehicle and license details, all types of offences, compounding amount, challan types, vehicle details, court calendar etc. in order to minimize the typing by the prosecuting officer.
7. The HH device should be able to access data/ information on the basis of driving license number, vehicle registration number etc. from the main server data relating to previous offences.
8. The hand-held application software should also suggest date of challan, place of challan, name of the Court and court date etc. to further reduce typing by the officer. These fields should be designed in consultation with Varanasi Traffic Police.
9. When a challan is issued, the name and ID of the officer should be printed on the Challan.
10. The HH device must be able to input and print multiple offences on the same Challan
11. The HHD software must validate Challan fields automatically before the Challan is printed. The system must ensure that certain fields are properly completed before allowing the Challan to be printed.
12. When downloading application software or pop-up tables or lists to the HH, or uploading challan records to the Server, synchronization of HH system must be automatic, in order to minimize human intervention

13. Uploading data to the Database Server should be automatic in consistent manner.
14. The application should provide features wherein when a driving license/ vehicle registration number is entered, it should be able to pull from the server all the details relating to the driving license holder/ vehicle owner including history of previous offences.
15. Software should capture the list of documents seized during prosecution and such list must be reflected on the printed court challan.
16. The handheld application software shall allow the user to generate a summary report to facilitate evaluation of his daily work.
17. Once the Challan is complete and saved any further editing should not be possible unless so authorized by administrator.
18. Each hand-held device should be provided with original printed user manual and appropriate carry case for HH device with charger.
19. The application software should allow online payment though payment gateway
20. There should be automatic rejection of payment for the settlement of expired notices or challans. Partial payment of an offence must not be accepted by the system including previous violations fees.
21. The software should update DL/RC smart card with the booked offence.

Functional requirements of ANPR & Surveillance Cameras:

- ANPR camera will capture the vehicle registration number with details like parking lot number, Date & Time stamp of entry, Date & Time stamp of exit
- ANPR camera should be capable of reading any type of number plates and may use OCR for recognition
- The Camera should recognize other language numbers may be based on the font installation
- ANPR cameras to be installed in all parking locations. The vehicle numbers will be sent to command control center with details like Parking lot ID, Date and Time, Type of vehicle (More details if required)
- For multi-level car parking 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 city operation Centre.

- For multi-level car parking the system checks daily whether the vehicles that have entered the premises but are yet to leave. Thereby KSPMS can generate alert if any vehicle is overstaying in the parking lot over 24 hrs
- MSI can install appropriate surveillance cameras at entry and exit points, camera in each floor of multi-level car parking. The smart parking solution should retain videos of car entering /exiting the parking zone as per the security parameters defined.

Functional requirements of Speed Violation Detection System (SVDS)

- The speed violation detection system detects the over speeding vehicles and generate an automatic e-Challan for the over-speeding violation. The below figure shows the speed violation detection system installation
- The speed violation detection system captures speed of the vehicles which are passing through this system. The speed detection system detects speed of the vehicle and compares with the speed limit set in the configuration. If the actual speed of the vehicle is more than the speed limit, then it triggers the ANPR system to capture the number plate of the vehicle. Both the number plate and actual speed of the violated vehicle will be stored in the system. The system detects speed accuracy of 10% (+/-) of the actual vehicle speed.
- The number plate deciphered are stored in the deciphered database. The number plate not deciphered by ANPR system are stored in the non-deciphered database. Later the non-deciphered number plate is manually further classified into soiled, broken and vernacular number plate.
- All the deciphered number plate of violated vehicles e-Challans generated automatically. Non-deciphered number plate of violated vehicles e-Challans are generated manually.

Functional Specifications of Public Address System

1. The Public Address System (PAS) should be capable of addressing citizens at specific locations from the KICCC.
2. The proposed system shall contain an IP-based announcing control connected to the KICCC.
3. 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 PAS 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.

4. 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).
5. The MSI shall describe in detail the design, operational and physical requirements of the proposed public announcement system to demonstrate compliance with all the specified requirements of RFP.
6. PAS 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.
7. PAS master controller should facilitate multiple MIC inputs and audio inputs.

Technical Requirements of ITMS

Technical requirements of Adaptive Traffic Control System-

Traffic Sensor Appropriate camera based traffic sensors may be chosen to provide the operational levels and accuracy as required for successful function of the ATCS as per the SLAs defined.

Adaptive Traffic Control- Traffic Controller

Appropriate camera based traffic sensors may be chosen to provide the operational levels and accuracy as required for successful function of the ATCS system as per the SLAs defined.

Adaptive Traffic Control- Traffic Light Aspects

Key Features:

- lowest power consumption for all colors
- Meets or exceeds intensity, color and uniformity specifications
- Temperature compensated power supplies
- Uniform appearance light diffusing
- ITE products shall be Intertek/ETL/EN/Equivalent certified
- All units operate on AC or DC as the per the suggested solution by bidder

LED aspects:

- Red, Amber, Green-Full (300 mm diameter) : Hi Flux

- Red, Amber, Green-arrow (300 mm diameter): Hi flux
- Red, Green-Pedestrian (300 mm diameter):Hi Flux and Hi Brite
- Animated Pedestrian-Red and Green Animated c/w countdown (200 mm) Hi Brite with diffusions

LED Retrofit Specifications

- Power Supply : 230 Vac *10% and frequency 50*5Hz
- Standards : EN 12368 complaint
- Convex Tinted Lens : Available
- Fuse and Transients : Available
- Operating Temperature Range : 00 Celsius to 550 Celsius
- Turn Off/Turn On Time : max 75 milli seconds
- Total Harmonic Distortion : <20%
- Electromagnetic interference : Meets FCC Title 47, Subpart B, Section 15 Regulation or equivalent EN/IRC standard
- Blowing Rain/Dust Spec : MIL 810F complaint or equivalent EN/IRC standard
- Minimum Luminous Intensity : Red 250, Amber 250, Green 250 (Measured at intensity point) (nm)
- Dominant Wavelength (nm) : Red 630, Amber 590, Green 490
- Lamp conflict compatibility System : Compatible with lamp failure and conflict detection

Technical Requirements- Red Light Violation Detection Systems

S.No.		Description	
1		General	
	a	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 violation occurred).	
2		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	Video Resolution	2 Megapixels(1920X10180) or better HD camera
	e	Video	H.264
	f	Frame rate	Min. 30 FPS
	g	Normal Horizontal Field of View	at least 3.5 Mtr. (One lane)
	h	Typical Range	30 Mtrs. or better
	i	Operating Temp.	0 to 55 Degree C
	j	Auto Iris Control	Yes
	k	Protection rating	NEMA 4X / IP-66 rated
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 minimum 24 hour 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 0oC to 55oC.	
	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).	
	g	UPS Backup (of minimum 30 minutes) to be provided only for RLVD System	
4		Violation Transmission and Security	

	a	Encrypted data, images and video pertaining to Violations at the Onsite processing station should be transmitted to the VMC 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 VMC, and its access will protected by a password.
	c	The vendor shall ensure that the data from the onsite processing unit shall be transferred to VMC 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

Technical Requirements- Variable message sign boards

S.No.		Description	
1		Dimensions	3.0 mtr length X 1.5 mtr height X 0.2 mtr depth. (3000mm x 1500mm X 200mm)
2		Color LED	Full Color, class designation C2 as per IRC/EN 12966 standard
3		Luminance Class/Ratio	L3 as per IRC/EN 12966 standards
4		Luminance Control & auto Diming	
	a	Should be automatically provide different luminance levels but shall also be controllable from the traffic centre using software	
	b	Auto dimming capability to adjust to ambient light level (sensor based automatic control)	
	c	Photoelectric sensor shall be positioned at the sign front and sign rear to measure ambient light. Capable of being continually exposed to direct sunlight without impairment of performance.	
5		Contrast Ratio	R3 as per IRC/EN 12966 standard
6		Beam Width	B6+ as per IRC/EN12966 standards

S.No.		Description	
7		Pixel Pitch	20mm or better
8		Picture Display	
	a	At least 300mm as per IRC /EN 12966 standards	
	b	Full Matrix: Number of lines & characters adjustable, active area: 2.88mX1.2m at least	
	c	Synchronized Dot to Dot display.	
	d	Capable of displaying real time, customized messages generated by KICCC.	
	e	Special frontal design to avoid reflection.	
	f	Display shall be UV resistant	
9		Viewing Angle	B6+ as per IRC/EN12966 standard- Viewing angle shall ensure message readability for motorists in all lanes of the approach road
10		Viewing Distance	Suitable for readability from 150 Mtrs. or more at the character size of 240mm, from moving vehicles.
11	a	Self-Test	
	b	VMS shall have self-test diagnostic feature to test for correct operation.	
	c	Display driver boards shall test the status of all display cells in the sign even when diodes are not illuminated.	
	d	All periodic self-test results shall be relayed to the VMC in real time to update status of VMS	
12	a	Alarms	
	b	Door Open sensor to Inform Control room during unauthorized access	
	c	LED Pixel failure detection alarm	
13		Flicker	Refresh Frequency should not be less 90 Hz. No visible flicker to naked eye.
14		Multiple Data Communication interface/Ports	RJ45 Ethernet, RS232, RS 485, FC port and any other suitable
15		Communication (connectivity)	Wired/GPRS based wireless technology with 3G upgradable to 4G capability.
16		Ambient Operating Temperature	The system should be capable of working in ambient temperature range of -5 oC to 55oC.

S.No.		Description	
17		Humidity (RH)	Operating ambient humidity: 10% - 95% Rh or better.
18		Protection against Pollution/dust/water	Complete VMS should be of IP 65 protection level from front and IP54 from side and rear. As per EN60529 or equivalent Standard
19		Power	
	a	170-250V AC (more than 90% power factor) or DC as per equipment requirement.	
	b	Protection for overvoltage/ fluctuation/drop of the nominal voltage (50%) shall be incorporated.	
	c	The enclosure shall contain at least two 15 Amp VAC (industrial grade) outlet socket for maintenance purpose	
20		Power Back-up & its enclosure	UPS for 15 Mins power back-up with auto switching facility. The enclosure of UPS and battery should be pole mountable with IP 65 protected housing and lockable. Batteries with solar charging options can also be recommended as back up
21		Material for VMS frame	at least 2mm aluminum or non-corrosive, water resistant or better
22		Mounting, Installation and finishes	
	a	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. MSI shall be responsible to carry out the site survey to assess site requirement including pole height/suitable structure for VMS installation at various places in the city.	
	b	The mounting shall be capable of withstanding road side vibrations at site of installation.	
	c	It shall be provided with suitable walkway for maintenance access.	
	d	The sides interior and rear of enclosures shall be provided in maintenance free natural aluminum finish. All enclosure shall be flat and wipe clean.	
	e	Rugged locking mechanism should be provided for the onsite enclosures and	

S.No.		Description	
		cabinets	
	f	For Structural safety, the successful bidder has to provide structural safety certificate from qualified structural engineers approved/ certified by Govt. Agency.	
23		Wind Load	WL9 as per EN12966 to withstand high wind speeds and its own load.
24		Cabling, connections and Labelling.	
	a	All cable conductors shall be of ISI marked for quality and safety. It shall be of copper insulated, securely fastened, grouped, wherever possible, using tie warps approximately every 10-20 cms or cable trays.	
	b	All connections shall be vibration-proof quick release connections except for power cables terminating in terminal blocks, which shall be screwed down.	
	c	All terminal block shall be made from self-extinguishing materials. Terminations shall be logically grouped by function and terminals carrying power shall be segregated from control signal terminals.	
	d	All cables shall be clearly labelled with indelible indication that can clearly be identified by maintenance personnel using "As built: drawings".	
	e	Lightening arrester shall be installed for safety on each VMS.	
	f	The successful bidder has to provide safety certificate from qualified Electrical engineers approved/certified by Govt. Agency	
25		Local Storage in VMS	Embedded VMS controller should be capable to store at least 100 messages and symbols/pictograms to allow display to run in isolated mode on a predefined structures/ timings, in case of connectivity failure.

Technical Requirements- Speed violation detection camera specific details

S. No.		Description	
1		**Speed**	
	a	Unit of Speed Measurement	Kmph
	b	Speed detection system to Capture speed	250 Kmph +/- 5%

S. No.		Description	
	c	Speed Enforcement Technology	Radar
2		**Digital Camera/Automatic Number Plate Recognition(ANPR) camera**	
	a	Video Compression:	H.264
	b	Video Resolution	1280X720
	c	Frame rate	Min. 30 FPS
	d	Image sensor	Color, Progressive scan CCD 1/3"
	e	Exposure Control	Global shutter, software adjustable 1/30 s – 1/ 27700 s
	f	Day/Night Mode	Configurable day/night mode switching
3		**Lens**	
	a	Lens Type	5.2 – 58.8 mm with high precision motorized positioning
	b	Iris	Automatic motorized, programmable
	c	Focus	Automatic motorized, programmable
	d	Zoom	Automatic motorized, programmable
	e	Optical Filter	Switchable: All pass / IR cut above 850 nm
	f	ANPR Range	3 m – 20 m (10 feet – 65 feet)
4		**Illumination**	
	a	Type	High power IR LED, regulated
	b	IR Wavelength	850 nm
	c	Intensity	3 preconfigured modes (low, medium, high)
	d	Flash Time	Software adjustable, up to 950 µs
5		**Processing & I/O**	
	a	CPU	Minimum 1.6 GHz x86 processor
	b	Storage Memory	Storage for 7 Days violation data
	c	Operating System	Linux
	d	ANPR	ANPR software
	e	Communication Protocol	ARP, ICMP, TCP/IP, DHCP, NTP, FTP, HTTP, SMTP, RTP
	f	Communication Interface	100Mbit/sec, Ethernet
6		**Radar frequency**	
	a	Measurement Principle	Doppler-Radar
	b	Radar frequency	Approved frequency in India
	c	Direction Selectable	uni- or bidirectional

S. No.		Description	
	d	Normal Horizontal Field of View	at least 3.5 Mtr. (One lane)
	e	Operating Temp.	-20 to +55 Degree C
	f	Protection rating	IP67
	g.	Certification	CE, FCC, UL, cUL, C-tick, CB, VCCI
7		**Local 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
	c.	The system should be capable of working in ambient temperature range of -20 degree C to 55 degree C.	
	d	Lightening arrester shall be installed for safety of system (As per BIS standard IS 2309 of 1989).	
	e	The housing(s) should be capable of withstanding vandalism and harsh weather conditions and should meet IP66, IK10 standards (certified).	
8		**Violation Transmission and Security**	
	a.	Encrypted data, images pertaining to Violations at the local processing unit should be transmitted to the TCC electronically through wired/ 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 TCC, and its access will protected by a password.	
	c.	The vendor shall ensure that the data from the onsite processing unit shall be transferred to TCC within one day.	

Technical Requirements- e-Challan Handheld device

Core board	
Operating System	Latest Windows or Android OS
Processor	Min 1 GHz min.
Memory (Flash ROM)	Minimum 8 GB
RAM	1 GB Min

Extend Slot	Micro SD 32 GB
Motherboard	
Display	Minimum 5.5 inch IPS, 1280*720 res.
Touch Screen	Yes
Form Factor	Yes
GPS	GPS/Galileo/Glonass/Beidou
Connectivity	4G/LTE/3G/2G/WiFi/Bluetooth
Smart/Magnetic Card Reader	Support
QR Code Reader	Camera/QR Code Reader
Mini-USB Connector	USB2.0 connection minimum
SIM card slot	Yes
TF card slot	Yes
Power jack	Yes
Audio Jack	Yes
Thermal Printer	Printing of minimum 2 inch in width
Barcode scanner	1D and 2 Scanner
External Interface	USB HOST/RS232(Customized)
Protection class	IP54
Drop resistance level	2m
Camera	
Camera	5 MP min (Auto focus)
Touch Screen	Support still image and video capture
Keypad	
Front	Touch screen/ On screen Keys
Battery	
Type	rechargeable Li-ion battery 2000mAh, Minimum Working Hours- 10 hrs
Operating & storage temperature	-5℃ to 50℃
Operating Humidity	10% - 80%
Weight	Maximum 550 g
Payment PINPAD	The device should have lPCI , EMV certified PINPAD as per RBI guideline for accepting payment through Credit / Debit card

Field Junction Box

S. No.	Parameter	Minimum Specifications
1	Size	Suitable size as per site requirements to house the field equipment
2	Cabinet Material	Powder coated CRCA sheet/ Stainless steel
3	Material Thickness	Min 1.2mm
4	Number of Locks	3 way lock
5	Protection	IP65, Junction Box design should ensure to keep the temperature within suitable operating range for equipment's and should also avoid intentional water splash and dust intake. Should have built in surge protection.
6	Mounting	On Camera Pole / Ground mounted on concrete base
7	Form Factor	Rack Mount/DIN Rail
8	Other Features	• Rain Canopy, Cable entry with glands and Fans/any other accessories as required for operation of equipment's within junction box. • Shall have separate inlet/outlet and 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.

Poles for camera (existing structures / poles can't be used)

S. No.	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	5-10 Meters, as-per-requirements for different types of cameras

S. No.	Parameter	Minimum Specifications
		& Site conditions
3	Pole Diameter	Min. 10 cm diameter pole (bidder to choose larger diameter for higher height)
4	Cantilevers	Based on the location requirement suitable size cantilevers to be considered with the pole
5	Bottom base plate	Minimum base plate of size 30x30x1.5 cm
6	Mounting facilities	To mount RLVD Cameras, CCTV cameras, Traffic Signals, Pedestrian Signals, Switch, etc.
7	Pipes, Tubes	All wiring must be hidden, through tubes/pipes. No wires shall be visible from outside.
8	Foundation	Casting of Civil Foundation with foundation bolts, to ensure vibration free erection (basic aim is to ensure that video feed quality is not impacted due to winds in different climatic conditions). Expected foundation depth of min. 100cms. Please refer to earthling standards mentioned elsewhere in the document
9	Protection	Lightning arrester at select sites as per the requirements

Edge Level Switch (at Traffic Junctions)

Sr. No.	Item	Specifications
1	**General Features**	The switch should be Industrial Grade ruggedized in nature that provides minimum 8 x 10/100/1000 BASETX access ports, additional 2 x 1000 Base-X SFP & 2x 1GE Uplink ports. One (1) ruggedized single mode SFP should be supplied with the switch.
		The switch should have non-blocking wire-speed architecture with support for both IPv4 & IPv6 from day one with wire-rate switching fabric of minimum 16 Gbps or more. Switch should have minimum 1GB RAM/DRAM & 1GB removable flash card.

		The switch should support backup storage drives, which will store the last known configuration of the switch, in the case of hardware failure and replacement. Reinserting the storage drive should restore the switch to original working condition without any manual intervention.
2	**Layer 2 Features**	802. 1Q VLAN on all ports with minimum 10k MAC address
		Spanning Tree Protocol as per IEEE 802.1d, ring protection protocol like REP or equivalent
		Should support Jumbo frames up to 9000 bytes & Link Aggregation Control Protocol (LACP) as per IEEE 802.3ad.
		The switch should support IGMP v1/v2/v3 &up to 1000 IGMP groups as well as IGMP snooping & IGMP filtering. Should also support MLD v1/v2.
3	**Layer 3 Features**	Static, Inter-VLAN routing must be enabled from day one
		The switch should support Dynamic Routing – RIPv1/v2, OSPF for both IPv4 & IPv6, PBR, network address translation etc. protocol by enabling/upgrading the license as & when required.
4	**Quality of Service (QoS)**	Switch should support classification and scheduling as per IEEE 802.1P on all ports with minimum four egress queues per port
5	**Features**	The switch should provide traffic shaping and rate limiting

IP Amplifier

S.No.	Description	Minimum specifications
a	Amplifier Type	Class D

b	Amplifier output	50 Watts
c	Connectivity	IP-POE based
d	Power	Automatic on/off operation
e	Operating temperature	-25°C and +55°C at a maximum relative ambient humidity of 95%.
f	Certification	CE
g	Monitoring functionality	Line monitoring
h	Environment protection	IP 55 or better

Public Address System

Sr. No.	Parameter	Specifications
1	PAS system	a) Should have the capability to control individual PAS i.e. to make announcement at select location (1:1) and all locations (1: many) simultaneously. b) The PAS should also support both Live and Recorded inputs.
2	Speaker	Minimum 2 speakers, To be used for Public Address System
3	Connectivity	IP Based
4	Access Control	Access control mechanism would be also required to establish so that the usage is regulated.
5	Integration	With VaMS and Command and Control Center or any other component if required
6	Construction	Cast Iron Foundation and M.S. Pole, Sturdy Body for equipment
7	Battery	Internal Battery with different charging options (Solar/Mains)
8	Power	Automatic on/off operation
9	Casing	IP-55 rated for housing
10	Operating conditions	0° to 50°C

City Surveillance System

KPIs for City Surveillance

Following CCTV Surveillance KPIs are to include the following:

1. City Surveillance should cater to an effective Monitoring and Management with appropriate decision support mechanisms.
2. City surveillance must ensure a pro-active 24*7 monitoring of PAN city parameter that capture video footages of all junctions across the road network of Varanasi and project the feeds to the proposed Command and Control center without time lag on real time basis.
3. City Surveillance System must ensure and provide a secure and safe environment for the citizens with intelligent and effective use of video analytics and integrated platform for all concerned departments.
4. The surveillance prime equipment i.e. High Definition Camera units which includes Fixed box, Domed, PAN-Tilt-Zoom, MultiSensor cameras must be located at a suitable position or vehicle wherein the required area is properly captured. The intensity of captured footage should be enough to sustain the clarity as per the required zooming levels. Industry leading practices must be adopted during the implementation phase w.r.t positioning and mounting the cameras, poles and junction boxes.
5. The surveillance system shall be to provide proactive security as opposed to reactive security on PAN city basis with a clear defined objective of each HD camera unit.
6. The surveillance System shall provide inter-operability of hardware, operating system, software, networking, printing, database connectivity, reporting, and communication protocols.
7. It has to be ensured that the pole is well placed for vibration resistance adhering to the road safety norms. Also, the poles erected to mount cameras are good, both qualitatively and aesthetically.
8. Appropriate branding/ color coding of junction boxes should be done, to warn mischief mongers against tampering with the equipment at the junction with the needful operational equipment. Cameras needs to be protected from the on field challenges of weather, physical damage and theft.
9. This City Surveillance software should have the capability to provide various alarms & triggers. The required analytics and related triggers should include Parking Violation, Wrong Direction, People loitering, Camera Tampering (In case this is an inherent feature of the camera, this may not be provided as a separate line item in VA), Unattended Object, Crowd detection, Traffic flow/Congestion, Traffic Volume estimation and statistical counts, Video Content Analytics Requirement, People tracking.
10. Video Management System must allow users to view a count of analytics events on the video pane while video is being displayed.
11. Each intersection should be fitted with outdoor cabinets dimensioned to host all equipment necessary to operate enforcement systems and traffic surveillance systems
12. The data retention of minimum 30 days has to be maintained at Command and Control Centre.

13. The city surveillance system must ensure real time and event base monitoring of the city, situation/ rule based alerts including early warnings for prevention and avoidance of unwanted incidents like riots, flooding, etc.
14. The system should support automated response based on events including communication of alerts to relevant authorities like Fire, Hospitals, etc. for swift response in case of emergencies.
15. The system should have access to historic video data for investigative purposes.
16. IP based Public Address System shall also be installed as part of the information dissemination system at various locations in the city. These systems shall be deployed at identified junctions to make public interest announcements.

Functional Specifications of CCTV Surveillance system

General Requirements:

- All CCTV hardware products (Model wise) offered in the project should be min UL, CE, FCC, RoHS certified.
- The OEM should have existence in India for more than 5 years in similar projects. (Under Companies Act, 1956/2013) in India.
- The OEM for CCTV Camera should have technical support presence with it's employees on its payroll in India. This is to justify will ensure long term after sales support & spare support from the OEM. Bidder to produce documentary proof to establish the eligibility.
- The OEM should have CMMI certification.
- OEM Should be in the well repeated in Video surveillance equipment manufacturing and deployment
- Local Service/support must be required.

Functional Requirements:

1. Varanasi City Surveillance System shall consist of:

   Fixed Cameras.

   - PTZ Cameras.
   - Network Video Recorder (IP BASED NVR).
   - Video Management System (VMS) including central software application.
   - Camera Accessories i.e. Power Supplies, Cable, Connectors and associated accessories for an integrated system.
2. The cameras implemented as part of this project shall be rated for operations in outdoor environment (for outdoor installations) and depending on the objective/application, shall be of different configurations including PTZ or fixed cameras.
3. All the Cameras shall be IP based.

4. The CCTV surveillance system shall be ONVIF compliant.
5. Cameras shall have an integral receiver/driver that shall be capable of controlling pan-tilt, zoom and focus locally and also remotely from the KICCC.
6. All cameras shall support real-time video content analysis.
7. The surveillance system shall support following Built-in-Analytics for the Cameras:
    - Perimeter Detection/ Intrusion – Virtual Tripwire
    - Auto-tracking for Facial Recognition - To detect and track movement in the field of view
    - Facial Recognition
    - Congestion Detection/People Counting/Crowd Gathering
    - Counter Flow and Movement/ Wrong or One way detection
    - Camera Vandalism - Triggers an alarm if the lens is obstructed by spray paint, a cloth or a lens cap.
    - Parking Violation
    - People loitering within restricted area
    - Left/Unattended Object - To detect objects placed within a defined zone and triggers an alarm if the object remains in the zone longer than the user-defined time allows
    - Object Classification
    - Stopped Vehicle: - To detect vehicles stopped near a sensitive area longer than the user-defined time allows.
8. Event (alarm) Handling: -
    - The camera shall be capable of recording an event as pre and post event images to on-board SD Media Card and on IP BASED NVR. Events may be triggered using camera motion detection or from an external device input such as a relay.
    - When triggered from an external input or the camera's motion detector, the camera shall be capable of sending JPEG images via e-mail and/or sequences of images to an FTP server or on-board compact flash and IP BASED NVR.
    - A relay output shall be available upon the activation of the camera's motion detector or external relay input. The relay output may also be manually activated from the live view screen.

9. Integration required with existing CCTV cameras deployed and functioning at important locations such as Hospitals, Schools, Market Places, etc. (actuals will be notified later) across city.

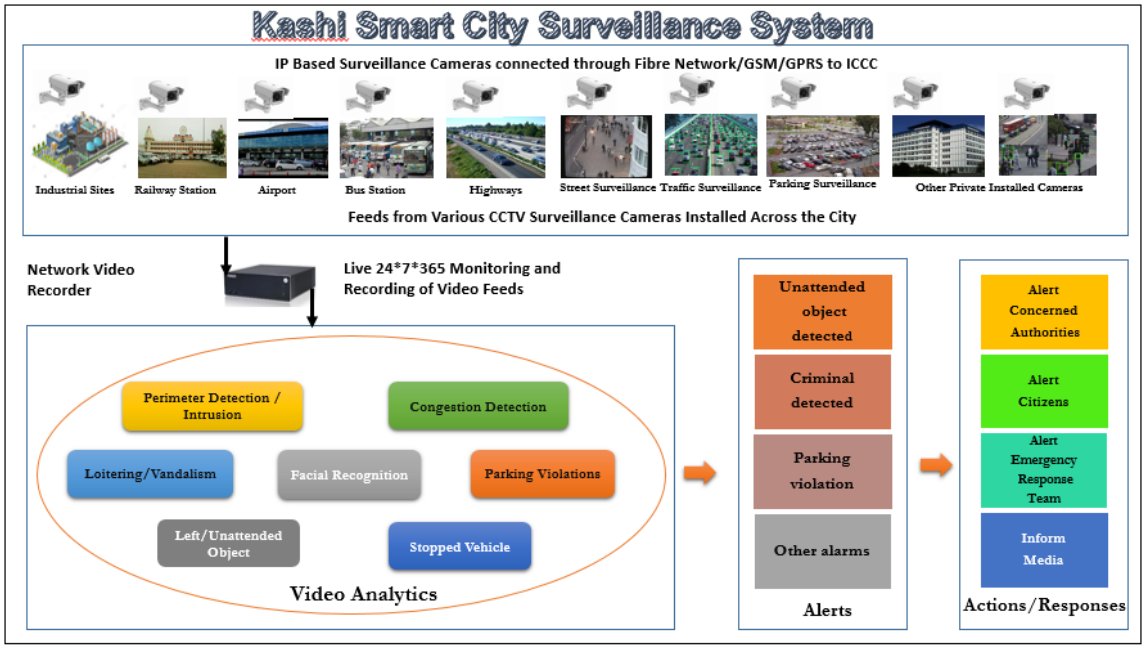


Figure : Illustrative Representation of Kashi Smart City Surveillance System.

Functional Specifications of Network Video Recorder (IP BASED NVR)

1. IP BASED NVRs shall be sized to provide minimum 30 days storage assuming recording of 24hrs a day, 7 days a week and 30 days a month at 4 CIF resolution. All IP BASED NVRs shall be provided in an N+N configuration.
2. IP BASED NVRs shall have in-built capabilities of recording video and audio streams directly from IP based cameras installed at field.
3. IP BASED NVRs shall be ONVIF compliant.
4. IP BASED NVRs shall be capable of reviewing video and audio streams on-demand using the supplied central software.
5. IP BASED NVRs shall be capable of storing all alarms generated as part of the CCTV surveillance system.
6. IP BASED NVRs shall be capable of supporting all recording of camera analytics.
7. IP BASED NVRs shall be network enabled for remote access, viewing, management and status monitoring. User Name and Password protection is required for access. The system must provide for remote administrator management of user names, passwords and management of definable end user rights.

8. A network user/client interface software shall be supplied at no cost to VSCL. The functional requirements of this client interface software will be reviewed and approved by VSCL or their designate.
9. IP BASED NVR Unit(s) shall provide fully configurable recording options to include, but not limited to:
    - Full record
    - Record on motion only
    - Variable frame rate
    - Variable resolution
    - Change of recording configurations on receipt of an alarm globally and/or per camera
    - Enable audio recording on receipt of an alarm

Functional Specifications of IP Based Video Management System (VMS)

1. Central software application to be installed at the KICCC shall be able to run on any PC based on standard operating systems and shall be license free.
2. Video Management System (VMS) shall be non-proprietary and open ended to support integration with KICCC platform.
3. Central Application Server shall allow user to view live video stream.
4. Software shall consist of a single client application and the client software shall not be dependent on, nor require any connection to, a central management or configuration server.
5. The client software shall be installable without any need for software or hardware license.
6. Dockable windows shall include:
    - Site Explorer
    - Alarms/Events window
    - PTZ and advanced telemetry functions
    - Monitors window
    - Maps window
7. The system shall support a distributed architecture with no single point of failure.
8. Video shall normally stream direct from camera to client; streaming via a proxy, or intermediate server shall not be the normal function of the system but may be selected as an option.
9. A client need not ask "permission" to connect to a camera. The handshake between client and camera shall be done directly.
10. There shall be no single management server. System management shall be distributed throughout the system.

11. Recording failover shall be standard without need for additional license and/or hardware.
12. BSCL's workstations must remain "connected" to all recording devices simultaneously.
13. Video shall normally stream direct from camera to client; streaming via a proxy, or intermediate server shall not be the normal function of the system but may be selected as an option.
14. Recording failover shall be standard without need for additional license and/or hardware.
15. VMS shall allow the overlay of time and date and site information on live video panes, either on all panes, or selected pane only. In addition, the overlay may consist of a user-provided transparent PNG or JPEG file.
16. VMS shall allow users to view live video and review recorded video at the same time.
17. VMS shall be ONVIF compliant.
18. Users shall be able to display any camera view (virtual preset).
19. VMS shall allow users to reveal the hidden zone in live video if the user has the appropriate permission.
20. Users shall be able to save the current zoom/scroll position as a camera view (virtual preset).
21. Administrators shall be able to configure hidden zones on fixed cameras.
22. VMS shall allow the display of analytics levels on video.
23. Users shall be able to take a snapshot of one image or all images currently displayed and save as a bitmap or JPEG image to a configurable location. This should include zoomed images.
24. Users shall be able to print a snapshot of an image displayed in a video pane direct on a printer (color or grayscale, depending on printer).
25. Users shall be able to replay currently viewed live video by a single mouse click for replays from 10, 15 or 30 seconds before current time or from alarm time.
26. Users shall be able to configure the size for text and icons displayed on video panes. Text and icons can be fixed size or adjust automatically when video pane size changes.
27. In the event of the video connection failing, the Video Management System shall display a clear error message with the option to also display the last video frame received.
28. Event Counting: The Video Management System shall allow users to view a count of analytics events on the video pane while video is being displayed. The Video Management System shall allow users to reset the event count for a camera.
29. Live Video on Analog or Digital Monitors: -
    - The Video Management System shall be able to display camera information in the On Screen Display (OSD) like Camera name, Date and time.
    - The Video Management System shall support point to point connections for the following data like Video (SD only), Audio transmit and receive, Serial
30. **Audio in Live Video**:
    - Users shall be able to listen to audio from multiple cameras through PC speakers.

- Users shall be able to speak to one or more cameras through a PC microphone.
- Users shall be able to listen to audio from a camera through monitor's speakers.
- Users shall be able to speak to a camera displayed on monitor through a microphone connected to a decoder.
- Users shall be able to mute a client speaker.
- The Video Management System shall have an option to allow or prevent simultaneous listen and speak (full duplex audio). If full duplex audio is off, the direction of audio will be switched automatically when the user listens or speaks.
- Users shall be able to listen to audio streams that do not have associated video.

31. **PTZ Control**:
    - All PTZ control shall be user-restricted.
    - Users shall be able to configure named preset positions with optional "tool tip" text.
    - Users shall be able to configure named custom commands with optional "tool tip" text.
    - Commands can be per PTZ type or per camera, as required.
    - Users shall be able to copy custom PTZ commands from one camera to another pane
    - Users shall be able to zoom a PTZ camera in or out using the PC mouse.
    - Users shall be able to simultaneously pan, tilt and zoom a PTZ camera displayed in a video pane or monitor using a joy stick on one of the supported CCTV keyboards.
    - Users shall be able to adjust the focus of a PTZ camera using the on screen PTZ controls or a CCTV keyboard.
    - Users shall be able to adjust the iris of a PTZ camera using the on screen PTZ controls or a CCTV keyboard: Open iris-Close-Auto-iris.
    - Users shall be able to move a PTZ camera to a preset position using the on screen PTZ controls or a CCTV keyboard.
    - Users shall be able to perform a custom command on a PTZ camera using the on screen PTZ controls (e.g. operate wipers.).
    - Users shall be able to enter the menu on a PTZ camera using the on screen PTZ controls or a CCTV keyboard (menu options navigated using pan and tilt.).
    - The Video Management System shall automatically drop the connection to a PTZ camera if not moved for 5 seconds to allow other users to control it.
    - Users shall be able to hold onto connections to PTZ cameras to prevent other users taking control if not moved (overrides the 5 second timeout.).
    - Users shall be able to take control of a PTZ camera if user has a higher priority than the user currently moving it (overrides PTZ hold.).

- Inform user when can't take control of a PTZ camera because another user with a higher priority is controlling it.
- Users shall be able to show or hide the on screen PTZ controls.

32. **Timeline and Calendar**:
    - Users shall be able to view the recorded video footage for a camera along a timeline. They shall be able to expand and contract the timeline to show a larger or smaller time range and to scroll the timeline backwards and forwards to show different time periods.
    - For a camera, users shall be able to see summary information about how much recording footage is available from which IP BASED NVR.
    - Users shall be able to change the playback IP BASED NVR associated with a camera.
    - The Video Management System shall provide one-button click controls to go to the beginning or the end of available recording footage.
    - The Video Management System shall provide a calendar control to allow navigation to any year / month /day in the recording library.
    - The Video Management System shall provide a go to "hour / minute / second" control.
    - The Video Management System shall display alarms related to the selected camera along the timeline including summary counts of the number of alarms in each time period.
    - The Video Management System shall display video bookmarks along the timeline. Bookmarks can either be those from a selected camera or from current bookmark query as displayed in the bookmark list.
33. **Playback on PC Screen or Video Wall**:
    - The Video Management System shall play back video recorded in MJPEG, MPEG4 and H.264 formats.
    - The Video Management System shall replay footage in same video pane, or navigate to recorded video panes.
    - The Video Management System shall play back video from up to 25 cameras at once in a single video window.
    - The Video Management System shall play back each camera separately or synchronize to playback from the same time.
    - The Video Management System shall play back synchronized recorded audio in each video pane.
    - The Video Management System shall display time and date information on recorded video panes, either on all video panes, or on the selected pane only. This should be able to be set independently of the settings for live video panes.

- The Video Management System shall play back video using the following standard VCR operations like Play-Pause-Fast Forward-Rewind at different speeds, Single Frame Forward, Single Frame Back.
- The Video Management System shall provide a jog shuttle speed control for fast forward and rewind.
- Users shall be able to move playback to a different time either using the timeline or entering a specific date and time.
- Users shall be able to move playback to the time of the next alarm, bookmark or motion over threshold.
- Users shall be able to move playback to the time of the previous alarm, bookmark or motion over threshold.
- Users shall be able to digitally zoom up to 1000% and scroll replayed video.
- Users shall be able to reveal the hidden zone in recorded video if user has the appropriate permission.
- Users shall be able to remove interlacing artefacts from 4CIF video.
- Users shall be able to display analytics levels on video.
- Users shall be able to take a snapshot of one image or all images currently displayed and save as a bitmap or JPEG image to a configurable location. This should include zoomed images.
- Users shall be able to print a snapshot of an image displayed in a video pane direct to a printer (color or grayscale, depending on printer.).

34. **Motion Search**:
    - Users shall be able to find motion in recorded footage from a selected time and display a motion profile on the timeline.
    - Users shall be able to adjust the motion threshold used for thumbnails and for moving playback to next/previous motion.
    - It shall be possible to combine motion search modes to further refine the search.
    - Users shall be able to adjust the speed and granularity of the motion search.
35. **Audio Search**:
    - Users shall be able to search for sounds in recorded footage from a selected time and display an audio level profile on the timeline.
    - Users shall be able to adjust the audio threshold used for thumbnails and for moving playback to next/previous sound.
36. **Thumbnails**:

- The Video Management System shall be able to display thumbnail images taken from the video footage in the current time line period. Thumbnails can be displayed by:
  a) Time: At equal intervals across the timeline period depending on the number of thumbnails set for the user.
  b) Alarms: One image for each alarm in the period.
  c) Bookmark: One image for each bookmark in the period
  d) Motion: One image for each time motion goes above a configurable threshold
  e) Audio: One image for each time the audio goes above a configurable threshold
  f) Users shall be able to play back a recording from a selected thumbnail

37. **Bookmarks**:

- Users shall be able to add a bookmark to a recording for a camera at a specified time.
- Users shall be able to find bookmarks by Site name, Camera name, Time range, text string within the bookmark.
- Users shall be able to produce reports of bookmarks and export to RTF, CSV or PDF formats.
- Users shall be able to delete one or more bookmarks (if created by the same user).
- Users shall be able to delete bookmarks created by any user.
- The Video Management System shall ensure that bookmarks are held alongside recordings on the IP BASED NVR, not on a user's PC.
- Users shall be able to view recorded video associated with a bookmark.
- It shall be possible for text information to be automatically fed into the IP Video System as bookmarks via an SDK.
- The Video Management System shall ensure that the text information is displayed in a scrolling bookmark comments window beside the playback window.
- Detailed search options shall allow for filtering of bookmarks e.g. by time, by user.
- Within the bookmark comments window the highlighted bookmark shall correspond to the current playback position.
- Next and previous incident buttons shall automatically scroll the bookmark comments window keeping the highlighted text and associated video in synch.
- In a live view pane, users shall be able to add a bookmark to the recording of that camera.
- Users shall be able to view bookmarks as a transparent overlay on a live pane.
- The Video Management System shall support permissions for bookmarks so that only those users with the appropriate security level can view bookmarks created by users at the same level as them or below.

38. **Incident Export**:

- Users shall be able to export video clips from a selected camera or cameras within a site to a named incident.
- Users shall be able to select the start and end times of the export by clicking and dragging on the timeline.
- Time to export shall be no more than 30 seconds per hour of video recorded.
- Users shall be able to queue video exports to be performed as a background process.
- The Video Management System shall show progress and estimated time to completion in an export status window.
- Users shall be able to add additional clips to existing incidents.
- The Video Management System shall automatically digitally sign video clips on export.
- Users shall be able to protect the original recordings to preserve the evidence.
- Users shall be able to review incidents in a standalone incident player application, directly from CD.
- Users shall be able to play back incidents with all the playback operations provided by the full Video Management System application.
- Users shall be able to check and authenticate digital watermarks embedded within exported clips.
- The Incident Player application shall be able to be run at the same time as the main Video Management System application so that users can easily verify the success of an export.
- The Video Management System shall support the following ONVIF cameras and cameras streamed via Camera Gateway:
  a) Export of video recorded in MJPEG, MPEG4 and H.264
  b) Playback of exported video in exported player
- The Video Management System shall provide the option to include date and time on each frame of the recording when it is exported.
- Administrators shall have the ability to restrict the location that users may export video files to.
- Users shall have the ability to produce a simple easy to view video summary of an incident.
- Users shall have the ability to export all video associated with this summary.
- All video in this export should be fully watermarked.
- The GUI shall allow addition, removal and edit of clips involved in the summary. This editing should be done via GUI.

39. **Playback on Monitors**:

- Users shall be able to play back recorded video on monitor from a selected time.

- The Video Management System shall support basic play back operations on monitor like Play, Pause.

40. **Audio in Playback**:
    - Users shall be able to listen to audio recorded with video from all cameras being played back or selected cameras only.
    - Users shall be able to listen to audio streams without the need to display anything in the video pane.
    - The Video Management System shall support listening to recorded audio for 3rd Party cameras through ONVIF.
41. Users shall be able to start an instant recording from live video viewed in a video pane. They shall have the option to start recording video only or both video and audio.
42. Users shall be able to configure the recording schedule for cameras on IP BASED NVRs. Recording can be configured to be: 24/7, Timed (from minute to weekly schedules), on alarm or event.
43. Users shall be able to specify the transport protocol to be used for recording (TCP, UDP, and Multicast.).
44. Users shall be able to specify whether audio should be recorded with the video.
45. Users shall be able to specify whether the recording should be protected when an alarm or event occurs (from a specified time before the alarm/event.).
46. Users with appropriate permissions shall be able to enable or disable recordings temporarily.
47. Users shall be able to delete recording schedules.
48. Users shall be able to copy recording schedules from one camera to other cameras on the same or another IP BASED NVR.
49. Users shall be able to specify an alternative IP BASED NVR to record to during a video "lockout" for either a camera or a site. Lockout permission can be used to prevent all other users from viewing and recording from a selected camera or all cameras in a selected site.
50. The Video Management System shall support digital signing (watermarking) of recordings as they are recorded on the IP BASED NVR.
51. Users shall be able to find recordings within a specified time period.
52. Users shall be able to protect/unprotect recordings.
53. The Video Management System shall display a warning message if an IP BASED NVR is unable to retain the number of days recording for which it was configured.
54. The Video Management System shall support the configuration of failover IP BASED NVRs for each primary IP BASED NVR with the following options:
    - 1 to N: 1 primary IP BASED NVR can have one or more failover IP BASED NVRs
    - N to 1: multiple primary IP BASED NVRs can have the same failover IP BASED NVR

- Continuous recording to primary and failover IP BASED NVRs
- Recording to failover IP BASED NVR only when primary IP BASED NVR fails

55. The Video Management System shall automatically failover when a primary IP BASED NVR is down.
56. In addition, users shall have the option to manually failover, for example to allow for routine maintenance of a primary IP BASED NVR.
57. Users shall have the option to manually fail back to a primary IP BASED NVR, with the option to restore the recording configuration from the failover IP BASED NVR to the primary.
58. The Video Management System shall support binary inputs on IP Cameras, encoders, decoders and alarm panels.
59. The Video Management System shall support video loss alarm inputs.
60. The Video Management System shall support network loss alarm inputs.
61. The Video Management System shall support IP BASED NVR fault alarm inputs, including:
    - Raid degraded
    - License failure
    - Recording failure
    - Redundant power failure
    - Redundant network failure
62. The Video Management System shall support analytics alarm inputs, with separate events for each analytics filter.
63. The Video Management System shall support alarm inputs from 3rd party systems.
64. The Video Management System shall enable multiple alarm inputs (detectors) to be grouped into an alarm zone.
65. The Video Management System shall support inputs (detectors) that do not cause an alarm to be generated.
66. The Video Management System shall support 'AND' logic between detectors so that the alarm input is activated only when both detectors are activated with a defined time period.
67. The Video Management System shall support detectors that are activated and deactivated by different inputs e.g. activate on a binary input from one device and deactivate on a binary input from another device.
68. Users shall be able to dock the alarm viewing window below the Live View or Playback View windows.
69. Users shall be able to sort the alarm information in various ways by clicking on column headings.
70. The Video Management System shall support set and unset of alarm zones such that alarms are only generated when the alarm zone is set.

71. Users shall be able to configure the time schedule for each alarm zone – different start and end times for each day and multiple time periods per day.
72. Users shall be able to define specific dates and times within time schedules so that exceptions for holidays etc. can be specified.
73. The Video Management System shall enable the same time schedule to be applied to multiple zones.
74. Users shall have the option of restoring the previous view after an alarm has been cleared.
75. Users shall be able to manually set and unset zones.
76. Users shall be able isolate faulty alarm inputs (detectors) such that they do not cause false alarms. Users shall be able to easily identify which alarm inputs are isolated and the reason for isolation.
77. The Video Management System shall enable zones to be set and unset on an event.
78. The Video Management System shall enable detectors to be isolated and restored on an event.
79. Users shall be able to specify a priority for each alarm zone (1-10.).
80. Users shall be able to configure the alarm sound for all alarm zones in a site or for each alarm zone individually. Sound can be from any .wav file and can be sounded once or repeated while the alarm is active.
81. The Video Management System shall allow alarms to be configured to require text from a user at the point of acknowledging and at the point of clearing.
82. The Video Management System shall allow an alarm procedure document (.html, text or URL) to be associated with a site or to an individual alarm zone. This procedure document shall be displayed when an alarm happens.
83. Users shall be able to configure the actions that should be performed when an alarm occurs:
    - Show video from camera, camera view or salvo in specified monitors
    - Stop video when alarm cleared
    - Move camera to preset position
    - Send email to multiple recipients, with option to include snapshots
    - Perform a relay action automatically
    - Start recording one or more camera – records for specified duration
    - Auto-protect recording from a specified duration before the alarm
84. Users shall be able to configure a second authorizing user for alarm clearing and relay actions – second user has to enter a password to authorize these functions.
85. The Video Management System shall support the following for 3rd Party cameras through native protocols and / or ONVIF:
    - Motion detection events
    - Record on motion
    - Video loss

- Network loss
- Change video quality on event, including frame rate, resolution and bitrate

86. Users shall be able to configure an unlimited number of alarm groups each containing a set of alarm zones and/or detectors.
87. For each user or user group, it shall be possible to associate one or more video panes with each alarm group. This should also include analog monitors.
88. Users shall be able to choose a display mode for alarm video. As multiple alarms come in, the video can either be "cascaded" across the chosen viewing panes or "queued" behind the chosen viewing panes. As alarms are cleared, the associated video is cleared from the chosen viewing panes. Cascaded video can either remain in the same video pane until cleared, or can move to the first available pane as earlier alarms are cleared.
89. When all alarm video is cleared from a viewing pane the Video Management System shall display video and layout being viewed before any alarm was displayed.
90. The Video Management System shall clearly mark black screen monitoring viewing windows as being distinct from normal live view windows through background color and icon.
91. The Video Management System shall remove any black screen monitoring analog monitors from the normal site hierarchy.
92. The Video Management System shall have permissions to determine which users or user groups get access to which alarm groups and which windows are used to display alarm video.
93. Users shall be able to configure any of the available viewing panes or analog monitors as a spot monitor for viewing significant live footage.
94. The Video Management System shall provide a toolbar option on all live viewing panes to copy the current video stream into the spot monitor.
95. The Video Management System shall keep an audit record of what video was started and stopped in the spot monitor, by which user and what times.
96. The Video Management System shall allow the video sequence that was viewed in the spot monitor by a selected user in a selected time period to be exported as a single incident.
97. Users shall be able to review all video watched by a selected user in a selected time period in an incident player. The video should be played back as one sequence in a single video pane.
98. The Video Management System shall generate an alarm if any of the detectors within an alarm zone are activated.
99. The Video Management System shall not generate new alarms for subsequent detector activations within the same zone so that the user only has one alarm to handle.
100. The Video Management System shall alert new alarms with flashing icon and optionally a sound.
101. The Video Management System shall automatically perform the actions configured for the alarm zone or detector:

- Show video from camera, camera view or salvo in specified video panes or monitors
- Move camera to preset position
- Stop video when alarm cleared
- Send email to multiple recipients
- Perform a relay action
- Start recording one or more cameras
- Auto-protect recording from a specified duration before the alarm

102. When all alarm video is cleared from a viewing pane the Video Management System shall display video and layout being viewed before any alarm was displayed.
103. From a looped replay, users shall be able to quickly jump to continuous replay from the alarm time.
104. The users shall be able to display a map showing the location of the alarm.
105. Users shall be able to view pending alarms in a list ordered by priority and time.
106. Users shall be able to filter the alarm list to show alarms only from specific areas (sites and zones.).
107. The Video Management System shall be able to display alarm procedure document for the alarm.
108. The Video Management System shall allow users to acknowledge alarms, entering alarm response text as required.
109. The Video Management System shall allow users to edit the alarm response text at any time before the alarm is cleared.
110. The Video Management System shall allow users to clear alarms, entering alarm response text as required.
111. Users shall be able to find historical alarms matching specified criteria:
    - Alarm type
    - Alarm state (new, acknowledged, cleared)
    - From site(s)
    - From alarm zones(s)
    - User(s) who acknowledged or cleared
    - Time range
112. The Video Management System shall be able to escalate alarms to other user groups if the alarm is not acknowledged within a pre-defined time period.
113. The Video Management System shall be able to escalate alarms to other user groups if the alarm is not cleared within a pre-defined time period.
114. The Video Management System shall support different escalation time periods for different alarm priorities.
115. The Video Management System shall be able to propagate an alarm to other areas (zones) if the alarm is not acknowledged within a pre-defined time period.

116. Users shall be able to produce reports of historical alarms and events and export to RTF or CSV formats.
117. Users shall be able to authorize an alarm to be cleared, by a second user entering a password.
118. Users shall be able to view live or recorded video associated with the alarm.
119. The Video Management System shall ensure that alarms are held on an alarm server, not on a user's PC.
120. The Video Management System (VMS) shall support integration with external data sources. An external Data Source shall be defined as any text string up to 320 characters.
121. The VMS shall support up to 1 external data record every second.
122. The VMS shall support up to 2 million data records.
123. The VMS shall support the ability to search and filter data records using the following:
    - A partial text string to search data record
    - Source IP address of data
    - Name of Data source
124. The VMS shall allow for the association of data records with video data.
125. Integration shall be available via a freely available open interface. The interface shall be via a software development kit.
126. Users shall be able to configure relay actions using binary outputs on IP Cameras, encoders and decoders.
127. Users shall be able to configure relay actions using external outputs to 3rd party systems.
128. The relay activation shall be pulsed with a configurable pulse time period.
129. The Video Management System shall support latched relay outputs.
130. Users shall be able to associate relay actions with specific cameras so that the actions are readily available when video is displayed from that camera.
131. The Video Management System shall perform relay actions on alarm and event.
132. The Video Management System shall be able to perform relay actions on a time-schedule.
133. The Video Management System shall automatically check for devices not on the network and notify users when not available.
134. It shall be possible to define the users who get notified if devices become unavailable.
135. Users shall be able to manage the bandwidth used for network scans by configuration of:
    - Monitor period (mins)
    - Minimum check interval (msec)
    - Perform fast check on log in
    - Perform fast check on refresh

136. The Video Management System shall scan for devices using any combination of IP broadcast addresses, individual IP addresses or ranges of IP addresses.
137. Users shall be able to turn off scanning of devices.
138. Users shall be able to set sites to offline mode. In this mode, all automatic communication with the site will be halted, while still allowing requested traffic.
139. Users shall be able to manually refresh any diagnostics view.
140. The Video Management System shall notify users when device times are not synchronized with the viewing PC (more than 60 seconds out).
141. The Video Management System shall notify users of problems with IP BASED NVRs. The notifications will be those supported by each IP BASED NVR.
142. Users shall be able to view the current status of an IP BASED NVR with visual indicators showing whether each item is OK or indicates problems:
    - Total disk space
    - Minimum free disk space
    - Used disk space (total – free)
    - Percentage space used (used disk space / total disk space)
    - License expiry date
    - Maximum streams
    - Maximum third party streams
    - Number of cameras recording
    - Number of cameras not recording
    - Number of recordings
    - Maximum recordings
    - Age of last deleted recording (indicates storage being achieved for each camera)
    - IP BASED NVR time
    - Any additional features supported by the IP BASED NVR.
143. Users shall be able to view per camera disk utilization for an IP BASED NVR. Display a list of cameras being recorded by an IP BASED NVR, showing the cameras with the highest disk usage at the top. Display the following info. For each camera:
    - Start time of first recording
    - End time of last recording
    - Total size of all recording
    - Total duration of all recordings
    - Recording rate (total size / total duration), in kbps

144. The Video Management System shall provide a support information tool, which gathers together log files and site database into a zip file.
145. Users shall be able to configure named user groups. A group can be granted administrator rights:
    - Full (can configure everything)
    - Restricted (can configure everything except users and groups)
    - No configuration rights (limited user functions only)
146. The Video Management System shall be able to hide administration options from normal users. The user interface shall be cleanly split into administrative functions and operational functions. Users who do not have administrative rights shall get a much simpler interface so that they are not confused by visible but disabled features.
147. Users shall be able to configure named user accounts and allocate them to user groups.
148. Users shall be able to enable and disable user accounts.
149. Users shall be able to set-up a user to use either machine OS standard authentication or a password when he logs into the Video Management System.
150. Users shall be able to limit the total number of video streams (live or recorded) that a user or member of a user group can display at once.
151. Users shall be able to limit the number of time-based thumbnail images that a user or member of a user group will display at once.
152. Users shall be able to allocate each user group or user a priority that is used when controlling PTZ cameras.
153. Users shall be able to grant global permissions to user groups or users (global permissions do not apply to specific objects such as cameras):
    - PTZ hold (allows a user to keep control of a PTZ camera when not moving it)
    - Video lockout (allows a user to perform a video lockout on any site of camera)
154. Users shall be able to grant permission for user groups and/or users to access any object in the system (sites, cameras, monitors, salvos, alarm zones, detectors and relays.) For each object access can be limited by function: -
    - List – see object in the user interface
    - View – view video from cameras, sequences, salvos and guard tours
    - Transmit audio (speak) to a camera
    - Playback recording from a camera or salvo
    - Record – make an instant recording of a camera
    - Export video clips or take snapshots from a camera
    - Control a PTZ camera
    - Display video on a monitor or video wall or activate a relay

- Respond to alarms from an alarm zone
- Hidden zone (live or playback) – access video behind a hidden zone
- Audio (live or playback) – receive audio from a device
- Set and unset an alarm zone
- Isolate and restore a detector
- Work offline
- Configure presets and access the camera menus

155. Users shall be able to reset access permissions on individual objects to use the access permissions of their parent site.
156. Users shall be able to configure application settings specific to each PC,
    - Enable or disable scheduled tasks
    - Enable or disable the application as the topmost window
    - Location for snapshot images
    - Format of snapshot image (bitmap or JPEG)
    - Folder for snapshot image
    - Replay incident in live or Playback view
    - Use software or hardware assisted video renderer
    - Use de-interlace filtering on live view by default
    - Use de-interlace filtering on playback by default
    - Set video de-interlacing
    - Enable or disable use of a CCTV keyboard
    - Serial port for CCTV keyboard
    - CCTV keyboard type
    - Video pane text scale factor (% of the default text size)
    - Resize text on video panes in proportion to video pane size
    - Video pane icon size (normal, medium, large)
    - Select icon size on video panes in proportion to video pane size
    - Date / time display on video panes (none, all, selected)
    - Load bookmarks on start up
    - Spot monitor (external monitor or specified video pane)
    - Protect recordings by default when exporting
    - Write date and time on exported recordings
157. Users shall be able to prevent simultaneous listen and speak (full duplex audio).

158. Users shall be able to configure the use of buffered playback when reviewing recordings.
159. Users shall be able to enable or disable alert messages.
160. Users shall be able to log into the Video Management System manually.
161. It shall be possible to start the Video Management System from the command line with the following options:
    - Username and password
    - Normal, full screen or video-only modes
    - Site database
162. The Video Management System shall allow users to log out and log in without closing the application.
163. The Video Management System shall have an option to require all users to re-enter their password when logging out.
164. The Video Management System shall remember display settings on a PC for each user at log off and restore settings at log in:
    - Which cameras are displayed in which video panes
    - PTZ controls displayed
    - Map window position
    - Alarm window position
    - Video window positions (default hidden)
    - Main window size and position and site explorer width
    - Recording calendar displayed
165. Users shall be able to change their own password (if given write permission to the site database).
166. Users shall be able to change their default location on the tree hierarchy.
167. Users shall be able to lockout all other users preventing them from viewing or recording video from a selected camera or all cameras in a selected site.
168. The Video Management System shall support an audit trail that can log user actions to an industry standard database e.g. SQL Server.
169. Users shall be able to specify the authentication method to be used between the client application and the audit trail database:
    - Local user password
    - Windows user password
170. The audit trail shall log the following user actions to the audit trail database:
    - User logged on
    - User attempted to log on and was denied access
    - User logged off

- User changed "home" site
- User acknowledged an alarm
- User cleared an alarm
- User received an alert message (e.g. device not available)
- User starting playing back a recording (forward)
- User started playing back a recording (backwards)
- User stopped playing back a recording
- User denied playing back a recording or playback failed
- User took control of a PTZ camera
- User released control of a PTZ camera
- Second user authorized relay action
- Second user authorized alarm to be cleared
- Second user denied authorizing a relay or alarm to be cleared
- Export recordings
- Protect recordings
- Manual start or stop recording
- User log out denied
- User starts playing live video from a specific camera
- User stops playing live video from a specific camera
- Creation, deletion or editing items stored in the Video Management System configuration database
- User created a bookmark

171. The audit trail shall log the following information for each entry in the audit log:
    - Date and time that the user performed the action
    - Name of the user performing the action
    - DNS name of computer running in ICOMC
    - The name of the application writing to the log
    - A string naming the type of action performed e.g. Log on
    - Name and matrix number of the object that the action applies to e.g. camera name and number
    - Further information about the action, in a structured form e.g.: "Alarm Time: 16-Feb-06 10:11:41, Alarm Response: False alarm"
    - Severity (applies to error message received log entry only)

172. The user shall be able to export a report from the audit trail database into a standard reporting tool, e.g. Excel.
173. The Video Management System shall discover IP Video devices on a network either by broadcast address or unicast addresses for each device.
174. The Video Management System shall allow configuration of IP Video System devices via their web configuration interface.
175. The Video Management System shall enable mass configuration of devices, in particular encoder settings on IP cameras and encoders.
176. Administrators shall be able to view video from each stream at the same time as making changes to the media parameters on an encoder to aid configuration.
177. Administrators shall be able to upgrade the firmware on IP Video System devices - multiple devices can be upgraded in one go.
178. Administrators shall be able to create a hierarchy of sites and sub-sites for organizing cameras and other items by location.
179. Administrators shall be able to set the time-zone on a site - different sites can each have their own time zone.
180. Users shall be able to reorder sites under their parent site (sites are ordered by number).
181. The Video Management System shall be able to automatically create a site hierarchy within a site database containing IP Video System devices visible on the network.
182. Users shall be able to create sequences and salvos within the sites, set up 24/7 recording for each camera and enable video loss and network loss alarms.
183. Users shall be able to add cameras, monitors, alarm panels, alarm servers and IP BASED NVRs to sites by dragging and dropping, selecting from a list or manually entering the IP Address and name.
184. Users shall be able to remove devices from sites.
185. Users shall be able to move devices, and other items such as sequences, salvos, and sub sites from one site to another by dragging and dropping.
186. Users shall be able to enter a localized display name for cameras, monitors, alarm panels, alarm servers and IP BASED NVRs which overrides the name stored on the device.
187. The Video Management System shall enable a copy of the configuration database to be cached locally on each user workstation to ensure continuity of operation when a connection to the central database is not available.
188. The Video Management System shall support a configuration database that is divided into multiple 'segments', e.g. one segment for each site. The Video Management System shall allow each segment to be configured and accessed independently.
189. The Video Management System shall support user access permissions so that only authorized users can access specific segments.

190. When the configuration database is divided into segments, the Video Management System shall allow all sites to monitored e.g. from a central monitoring facility.
191. Users shall be able to create one or more maps for each site by importing an image for the background. The following image formats shall be supported:
    - Bitmap (BMP)
    - JPEG (JPG)
    - Portable Network Graphics (PNG)
    - AutoCAD drawings (DWG)
    - GIS
192. Users shall be able to add links to other maps.
193. Users shall be able to reposition items by drag and drop or entering specific coordinates.
194. Users shall be able to add cameras to map via drag and drop.
195. Users shall be able to specify the field of view for each camera.
196. Users shall be able to add alarm zones and detectors to map.
197. For alarm zones, users shall be able to have options to not display the alarm icon and/or name unless the alarm is active.
198. For zones and detectors, users should be able to configure a detector/zone area on the map.
199. Users shall be able to specify the amount of detail displayed for each object including icons, matrix numbers and labels.
200. Color schemes shall be configurable to make text and fields-of-view more visible.
201. The map shall be fully scalable with zoom and pan supported under mouse control.
202. Users shall be able to displays the previous maps viewed (back, forward).
203. Users shall be able to link to any map from any map.
204. Users shall have the option of scaling icons to a fixed zoom level.
205. The map should be viewable on a separate monitor from the main video(s).
206. Users shall be able to display live and recorded video from any camera on a map (drag and drop).
207. Users shall be able to view video from some or all of the cameras on a map via drag-select.
208. Users should be able to click on the field-of-view of any camera to view the video.
209. Where fields-of-view overlap, clicking on the convergent area should result in all cameras being displayed.
210. Activated alarms shall be visually represented on the map.
211. Where detector/zones areas have been configured, these should be visually represented as being in an alarmed state.
212. Where detector/zones areas have been configured and in an alarmed state, the user should be able to start video from all cameras associated with that zone by clicking on it.
213. Users shall be able to:

- Manage alarms from a map
- Clear alarms
- Acknowledge alarms
- View Video associated with an alarm
- Isolate/restore alarms
- Set/unset detectors

214. Users shall be able to trigger events to binary outputs on cameras or encoders.
215. The Video Management System shall include a restricted access version of the video viewing and replay application that prevents all users from accessing the setup screens even if they have an administrator login.
216. The Video Management System shall provide a restricted access site database management utility, which prevents creation of new site databases.
217. The Video Management System shall provide a restricted access version of the video viewing and replay application, which prevents all users from modifying the audit log configuration even if they have an administrator login.

Functional Specifications of Video Display System

1. Shall view live or recorded video from resizable and movable windows
2. Should have an ability to perform video controls for video systems from workstation
3. Shall play, fast-forward, rewind, pause, and specify time to play recorded video
4. Shall take a video still image (snapshot) from live or recorded video
5. Shall export video for user specified time and duration
6. Shall have the capability to move PTZ cameras
7. Shall view Video in Video Matrix
8. Shall display in 1x1, 2x2, 3x3 and 4x4 window formats
9. Shall enable operator to specify video windows to be displayed in matrix
10. Shall enable matrix settings to be saved per user
11. Shall view either live or recorded video can be displayed in the video matrix window.
12. Shall enable video snapshot to be taken and saved from any window pane in the matrix view
13. Shall rotate video in "virtual" video guard tour
14. Shall rotate through multiple video views based on predefined video camera sequence and duration.
15. Shall enable the user to pause the rotation of video and resume the video rotation again
16. Shall enable times between new video to be adjusted
17. Shall enable both live video and recorded video to be played through the video guard tour.

18. Shall enable alarms to be generated from any video pane
19. Shall enable user to only view and control video for which they have been assigned permissions by the administrator
20. Shall manually create an alarm from the live or recorded video with specified severity and description.

Functional Specifications of Recording and Storage

1. The storage solution proposed is that the video feeds would be available for 30 days. After 30 days, the video feeds would be archived unless it is flagged or marked by the Police or VSCL for investigation or any other purpose. The video feeds of all relevant cameras capturing the incident in question would be stored until the Police or VSCL deem it good for deletion.
2. For incidents that are flagged by the Police, VSCL 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.
3. 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.
4. 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.
5. The system shall support H.264 or better, MPEG-4 and MJPEG compression formats for all IP cameras connected to the system.
6. The system should not limit amount of storage to be allocated for each connected device.
7. 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.

8. 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.
9. 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.
10. The Recording Server/System shall support Camera devices from various manufacturers.
11. The Recording Server/System shall support the PTZ protocols of the supported devices listed by the camera OEMs.
12. The system shall support full two-way audio between Client systems and remote devices i.e. CCTV.
13. 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.
14. SNMP Support - The system shall support Simple Network Management Protocol (SNMP) in order for third-party software systems to monitor and configure the system. The system shall act as an SNMP agent which can generate an SNMP trap as a result of rule activation in addition to other existing rule actions.

Functional Specifications of Video Analytics System

1. The Video Analytics shall be designed to provide Intelligent Video Analysis for 24/7 surveillance with support for devices from different vendors.
2. Support any architecture namely distributed, centralized and hybrid.
3. Support system openness without using any proprietary format.
4. Support commercial-off-the-shelf computing hardware without the need of any proprietary hardware.
5. Able to produce reliable analytics at lower resolutions like 4CIF resolution in order to save the computation.
6. Able to process at variable resolution and frame rate when if necessary.
7. It shall support open platform Video Management System (VMS).
8. It shall provide ONVIF (Open Network Video Interface Forum) device discovery.

9. It shall get video from camera or VMS and send alarms to VMS to be viewed in VMS client.
10. It shall stream the Analytics Video to VMS using open interface protocol like ONVIF.
11. It shall support multiple regions of analytics on single video feed.
12. It shall support multiple features to be enabled for each of the regions.
13. It shall support feature based scheduling so that that alarms can be enabled or disabled for a certain period of time.
14. It shall support both Virtual line and Virtual area based features. The virtual area can be of any shape and can be bound by at least 10 end points.
15. It shall support both indoor and outdoor environment.
16. It shall support setting of minimum and maximum object size for detection.
17. It shall support masking of area in a view.
18. It shall support object masking.
19. It shall support color detection for vehicle & Object.
20. It shall support alarms to filter based on object color, size, speed and aspect ratio.
21. It shall support analytics capability to run both on server as well as edge (on camera).
22. It shall support simultaneous running of different features both on edge as well as server for same camera.
23. Various video analytics that shall be offered on identified cameras but not limited to are:
    - Perimeter Detection/ Intrusion – Virtual Tripwire
    - Auto-tracking for Facial Recognition
    - Facial Recognition
    - Congestion Detection/People Counting/Crowd Gathering
    - Counter Flow and Movement/ Wrong or One way detection
    - Camera Vandalism
    - Parking Violation
    - People loitering within restricted area
    - Left/Unattended Object
    - Object Classification

Technical Requirements for CCTV City Surveillance

Technical Requirements- Fixed and PTZ Camera, Lenses and Mounts

1. The camera control shall comply with the latest release of Open Network Video Interface Forum (ONVIF) standards.

2. The camera shall include an integral receiver/driver. The receiver/driver shall be capable of controlling pan-tilt, zoom and focus locally and remotely from the KICCC.
3. The camera shall incorporate Automatic Gain Control (AGC) circuitry to provide for compensation at low light levels.
4. The lens shall be integrated with the camera.
5. The camera shall be capable to produce minimum 30 frames per second (fps).
6. The camera shall provide automatic white balance, automatic exposure, automatic gain control, electronic shutter, and backlight compensation.
7. The camera shall be a true day/night cameras with mechanical IR cut filter.
8. The camera shall be capable of providing a high contrast color picture with a full video output at a minimum illumination as mentioned in the specifications.
9. Automatic light range circuits shall be included to provide compensation for variations in scene brightness. The circuits shall provide pictures over a light range of 1 million to 1.
10. All cameras shall capture high definition video, compress the video using H.264 technique and transmit real-time using fiber optic based communications system.
11. The cameras shall capture audio and compress using G.711 technique and transmit real-time using fiber optic based communications system.
12. All cameras shall support on-board real-time video content analysis.
13. All cameras shall support both Constant Bit-Rate (CBR) and Variable Bit Rate (VBR) options.
14. The camera shall support up to 2 video profiles, each providing independent configuration of bit rate, frame rate and resolution.
15. The camera shall support video compression from 64kbps up to 10Mbps.
16. The camera shall support audio compression using the G.711 compression algorithm, streaming @ 32Kbps per channel sampled at 8 KHz or 16 KHz with a 16 bit resolution.
17. The camera shall support on-board storage via micro SDHC slot and card with a minimum capacity of 64 GB.
18. All cameras shall have integral in-built adaptive IR technology. For fixed cameras, the IR shall support a range of at least 50m and for PTZ it shall support a range of at least 200m moving with zoom (adaptive).
19. For Fixed Cameras:
    - The fixed camera shall provide a minimum focal length range of 2.8-10 mm compensated with a minimum 12x digital zoom and shall be remotely controllable from the camera control transmitter at KICCC.
    - The fixed camera shall capture video using 1/3" progressive scan CMOS or better.
    - Fixed Camera resolution shall be 2048 x 1536 or better.
20. For PTZ Cameras:

- Camera shall have capabilities of PAN of 360° continuous.
- Camera shall have capabilities of Tilt of 180°.
- Lens of 4.3mm-129mm with minimum 35X optical and 12X digital zoom.
- PTZ camera shall capture video using minimum 1/3" type CMOS sensor or better.
- It shall support resolution of 1920x1080 or better.
- Camera shall support tilt of 100° either side. The tilt capability shall include both the horizontal (level view) and vertical (downward view) position. If the camera travels beyond straight down, automatic image flip circuitry shall prevent the display of an inverted image.
- The pan and tilt mechanism shall be an integral part of the camera.
- Pan speed shall be between 0.1-350°/s and Tilt speed shall be 0.1-350°s.

21. There shall be a minimum of 100 assignable automatic preset positions.
22. There shall be a minimum of 8 definable privacy zones.
23. All cameras shall provide effective 24/7 imaging performance for CCTV surveillance applications.

All cameras shall provide user control, with remote configuration for functions including streaming and compression settings, exposure, white balance, flicker control, picture size, cropping/privacy, brightness, sharpness, saturation, day-night switching point, frame rate, image rotation, snapshot, dynamic bandwidth allocation and motion detection.

Fixed Camera with Outdoor Housing and Lens – 2MP

S#	Description	Required Parameters
1	Image sensor	1/3"Progressive Scan CMOS or better
2	Lens	CS Mount: 5-50mm, DC-Iris, Megapixel IR corrected Lens
3	True Day and Night	Yes
4	Minimum Illumination / Light Sensitivity	Color: 0.3 lux F1.4 B/W: 0.08 lux F1.4 or Better
5	IR Filter	Automatic Built in IR Cut filter
6	Shutter Speed	1s to 1/30000
7	Video Compression	H.264 High, Main, Base profile and MJPEG
8	Resolutions and frame rates (H.264)	1920 x 1080
9	Video Streams	Minimum 4 @ H.264, 2MP, 25 fps or better
10	Power Supply	Power over Ethernet (PoE) IEEE 802.3af Class 2

11	Pan/Tilt/Zoom	Digital PTZ
12	Digital I/O (Alarms)	DI x 1 DO x 1
13	Local storage	SD Card Slot with 128GB Support
14	Image Settings	Color, Brightness, Sharpness, Contrast, Whitebalance, Image Mirroring, Text and mageoverlay, Privacy mask, Rotation: 0°, 90°, 180°, 270°, Exposure control, Exposure zones, Fine tuning of behavior at low light, Mirror Image
15	Supported Protocol	IPv4 & v6, HTTP, HTTPS, SSL/TLS, QoS Layer 3 DiffServ, FTP, CIFS/SMB, SMTP, Bonjour, UPnP ,SNMPv1/v2c/v3(MIB-II), DNS, DynDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS, SSH
16	Security	IEEE 802.1x, IP Address Filter, Password Protection, Digest Authentication
17	ONVIF	Profile S & G
18	API	The interface shall be available for integration with 3rd party analytics and applications in public domain free of cost
19	Operating Conditions	- 10°C to 50°C, Humidity 10–100% RH (condensing)
20	Privacy Mask	Required with Minimum 2 Zones
21	Image Configuration	The camera allows include/ exclude area in any shape in order to redue false alarms and bandwidth/ storage
22	GOV Length	It is possible to vary the GOV length in the camera setting for better control on bandwidth
23	Wide Dynamic Range	Minimum 120 dB True or Better
24	Event Triggers	Motion Detection, Edge storage events, External Input, Time Scheduled, Camera Tamperring, Software alarms. The camera shall be able to send and received trigger directly from any other camera without interface of VMS.
25	Event Actions	FTP or HTTP or network share, EMAIL, Notification via HTTP to other camera or device, Pre and post alarm video buffering, External Output Trigger, PTZ Preset, Guard Tour

26	Firmware Upgrade	The firware upgrade shall be done though web interface, The firmware is available free of cost
27	Embedded Applications	The camera shall provide a platform allowing the upload of third party applications into the camera
28	Memory	512 MB RAM, 256 MB Flash with Support for Edge Based analytics from 3rd Party
29	Housing	IP 66 Rated IK 10 rated for outdoor use
30	Certifications	CE, FCC, IEC, EN, UL
31	Warranty	5 years OEM warranty

High Definition Fixed Camera

S#	Description	Required Parameters
1	Image Sensor	1/2.8" progressive scan RGB CMOS
2	Operating Frequency	50 Hz
3	Day/ Night Operation	Yes with IR Cut Filter
4	Minimum Illumination	Colour: 0.2 Lux @ 30 IRE B/W": 0.01 @ 30 IRE 0 Lux with Built in or External IR, IR Range 50 Meters
5	Low light Capability	The camera shall be able to provide usable Color video in low light conditions
6	Lens	8-50mm IR corrected, CS-mount lens, P-Iris
7	Electronic Shutter	1/28000 s to 2 s or better
8	Image Resolution	1920 x 1080, 1280 x 720, 800 x 450, 480 x 270, 320 x 240
9	Compression	H.264 in High and Base profile, MPEG4, MJPEG
10	Frame Rate and Bit Rate	25 FPS at all resolutions with Controllabe Bit Rate/ Bandwidth and Frame Rate
11	Video Streams	Minimum 4 Streams in H.264, 2MP, 25 fps
12	Motion Detection	Yes built in with multiple configurable areas in the video stream
13	Pan Tilt Zoom	Digital PTZ
14	Frame Rate and Bit Rate	Upto 50 fps at all resolutions
15	Electronic Exposure & Control	Automatic/ Manual

16	Wide Dynamic Range	120 dB or better
17	Backlight Compensation	Required
18	Privacy Masks	Minimum 20 configurable 3D zones
19	Connectors	1 Input & 1 Ouput for Alarm Interface
20	Audio	Two way Audio
21	Event Triggers	Intellignet video,Edge Storage event, External Input, Audio Level, Motion Detection, Day/Night Mode,Network, Time scheduled, 3rd Party Analytics, Manual Trigger, Alarm Input Trigger
22	Event Actions	File upload: FTP, HTTP, network share and email Notification: email, HTTP and TCP PTZ funtion, Edge Storage/ NAS Storage, Pre & Post Alarm Recording, Actions configurable by web interface, External Output activation
23	Edge Storage	Built in SD card slot with support upto 128 GB with Class 10 speed
24	Built in installation aids	Focus assistant, Pixel counter, Remote back focus
25	Storage	The Camers shall have the feature to directly record the videos/ images onto NAS/SAN without any Software or integration
26	Protocals	IPv4/v6, HTTP , HTTPS b, SSL/TLS b,QoS Layer 3 DiffServ, FTP , CIFS/SMB, SMTP, Bonjour, UPnP™,SNMPv1/v2c/v3 (MIB - II), DNS,DynDNS, NTP, RTSP, RTP,TCP, UDP,IGMP,RTCP,ICMP,DHCP,ARP,SOCKS
27	Text Overlay	Date & time, and a customer-specific text, camera name, graphical image etc
28	Security	Password protection, IP address filtering, HTTPS encryption, IEEE 802.1Xa network access control, Digest authentication, User access log
29	Firmware Upgrade	The firware upgrade shall be done though web interface, The firmware shall be available free of cost
30	Logs	The camera shall provide minimum 200 logs of latest connections, access attempts, users connected, changes in the cameras etc
31	Interface	RJ 45, 100 Base TX
32	Enclosure	IP66-and NEMA-4X-rated casing (polyester polycarbonate blend)
33	Power requirements	Vendor to Specify
34	Operating	-20 °C to 55 °C

	Temperature	
35	Operating Humidity	Humidity 10–95% RH (condensing)
36	Certification	UL, CE, FCC, IEC
37	Application Programmers Interface	The interface shall be available for integration with 3rd party analytics and applications in public domain free of cost
38	Housing, Mount and IR	Shall be of the same make of OEM or better
39	Onvif S	Required
40	Warranty	Min 5 Years OEM Warranty

High Definition PTZ Dome Camera

S#	Description	Required Parameters
1	Image Sensor	1/3" Progressive Scan CMOS or better
2	Operating Frequency	Min 50 Hz
3	Day/ Night Operation	Automatic with IR Cut Filter
4	Minimum Illumination	Colour: 0.3 Lux @ 30 IRE B/W": 0.01 @ 30 IRE or better
5	high-speed pan-tilt functionality	360° endless pan range and a 180° tilt range
6	Optical Zoom	30x Minimum & 12x Digital Zoom, Total 360x Zoom or better
7	Lens	4.3-129 mm or better
8	Pan, tilt, manual and preset speed The speed shall be applicable for Manual, Tour and Preset Mode	0.5° - 350°/s or better
9	Image Resolution	1920 x 1080 or better
10	Compression	H.264 Baseline, Main and High Profiles, Motion JPEG
11	Frame Rate and Bit Rate	25 FPS at all resolutions with Controllabe Bit Rate/ Bandwidth and Frame Rate. In CBR Priority to be defined for Video quality or frame rate and the bandwidth upper limit shall not exceed the defined limit
12	GOP/ GOV	Ability to change the GOP/GOV Length to optimize the bandwidth and storage

13	Video Streams	Minimum 4 Streams @ 1920x1080, H264, 25 fps
14	Motion Detection	Yes built in with multiple configurable areas in the video stream
15	Electronic Shutter	1/33000 s to 2 s or better
16	Electronic Exposure & Control	Automatic/ Manual
17	Wide Dyanamic Range	120 dB or Better
18	Backlight Compensation	Required
19	Electronic Image Stabilization	Required
20	Image Freeze on PTZ	Required
21	Privacy Masks	Minimum 10 configurable 3D zones or better
22	Preset Positions	Minimum 256 or better
23	Image Flip	Yes Automatic
24	Guard Tour	Minimum 2 Nos
25	Built In Heater & FAN	Required
26	Temperature Control	Required
27	Audio	Two Way
28	Alarm	4 Configurable Input/ Output Ports or better
29	On-screen directional indicator	Required
30	Compression	The camera shall for its H.264 implementation support scene adaptive bitrate control, in order to lowering bandwidth and storage requirements. The camera shall support automatic dynamic GOP for optimal bitrate utilisation.The camera shall support automatic dynamic ROI to reduce bitrate in unprioritized regions.
31	Event Triggers	The camera shall be able to send and received trigger directly from any other camera without interface of VMS. Live Stream Accessed, Motion Detection, Shock Detection, Audio Detection, Network, Temperature, Manual Trigger, Virtual Inputs, Alarm Inputs, PTZ: Error, Moving, Preset Reached, Ready, Storage Disruption, Storage Reocrding, System Ready, User schedule

32	Event Actions	File upload via FTP, SFTP, HTTP and email Notification via email, HTTP and TCP Pre- and post-alarm video buffering, External output activation, PTZ preset, guard tour, Video recording to edge storage, Day/night mode, Overlay text
33	Pixel Counter	Built in
34	Edge Storage	Built in SD card slot with support upto 128 GB with Class 10 speed
35	Storage	The Camers shall have the feature to directly record the videos/ images onto Nas without any Software
36	Protocals	At least IP, HTTP, HTTPS, SSL/TLS, TCP, ICMP, SNMPv1/v2c/v3 (MIB-II), RTSP, RTP, UDP, IGMP, RTCP, SMTP, FTP, DHCP, UPnP, ARP, DNS, DynDNS, SOCKS, NTP, CIFS/SMB. IPv4 & IPv6 and Bonjour
37	Text Overlay	Date & time, and a customer-specific text, camera name, graphical image etc
38	Security	Password protection, IP address filtering, HTTPSa encryption, IEEE 802.1Xa network access control, Digest authentication, User access log
39	Firmware Upgrade	The firware upgrade shall be done though web interface, The firmware shall be available free of cost
40	Logs	The camera shall provide minimum 200 logs of latest connections, access attempts, users connected, changes in the cameras etc
41	Interface	RJ 45, 100 Base TX
42	Enclosure	Die Cast Aluminium, IK10 rated, IP66 rated, polycarbonate clear dome and sunshield, PVC free complying to WEEE Standards
43	Mount	Wall / Pole Mount
44	Power requirements	Power over Ethernet Plus (PoE+) IEEE 802.3at Type 2 Class 4, max. 24 W, Typical 9W; 24 V DC max. 30 W 24 V AC, max. 40 VA or better
45	Operating Temperature	-25 °C to 55 °C or better
46	Operating Humidity	10–95% RH (condensing) or better
47	Certification	UL, CE, FCC
48	Embedded Applications	The camera shall provide a platform allowing the upload of third party applications into the camera

49	Application Programmers Interface	The interface shall be available for integration with 3rd party analytics and applications in public domain free of cost
50	Onvif	G and S required
51	Warranty	Min 5 Years OEM warranty

Multi Sensor 360° Panoramic View PTZ Camera

Sr. No.	Parameter	Minimum Specifications or better
1	General Requirements	The camera should be manufacturer's official product line designed for commercial / industrial 24x7x365 use. The camera and camera firmware should be designed and developed by same OEM.
2	General Requirements	The camera should be based upon standard components and proven technology using open and published protocols
3	Image Sensor	Minimum 4 x 3MP, 1/3.2" CMOS - (Total) 12MP or better
4	Lens Specs	F2.0, Day/night (infrared cut filter); Options of 2.8/4/8/12/16 MM wide angle Lens
5	Video Resolution	1920 X 1080 or better
6	Minimum illumination	Colour: 0.6 lux or better, Monochrome: 0.05 Lux or better with IR
7	Video Compression	H.264, Motion JPEG
8	Frame Rate	15fps or better
9	Wide Dynamic Range	100 dB or better
10	Camera Angle Adjustment	Pan: - ±90° Tilt: - 28° - 92° Rotate: - ±90°
11	Network Interface	100 Base-T ports
12	Power Supply	POE IEE 802.3af compliant
13	Industry Standards	ONVIF Compliant
14	Certifications	UL, FCC
15	Enclosure Type	IP66; IK 10
16	Operating Temperature	0° C to 50° C or better
17	Operating Humidity	0 - 90%
18	Supported Network protocols	Minimum of the following RTSP, RTP/TCP, RTP/UDP, HTTP, DHCP protocols to be supported

Sr. No.	Parameter	Minimum Specifications or better
19	Support	The system should not be an end of life / end of service product.

Technical Requirements- Network Video Recorder (IP BASED NVR)

1. The Network Video Recorder (IP BASED NVR) will be connected via a Gigabit Ethernet network.
2. IP BASED NVR shall be of N+N configuration..
3. All equipment shall be designed to provide a usable life of not less than 15 years.
4. The IP BASED NVRs shall have a self-diagnostic feature including disk status, CPU usage, motherboard temperature, network status and fan status.
5. The IP BASED NVRs shall be support interface using 10/100/1000BaseTX. It shall support a total throughput of at least 700 Mbps.
6. The IP BASED NVR shall be powered using 100-240VAC/50Hz.
7. Each IP BASED NVR unit shall be maximum of 2U height.
8. The IP BASED NVR shall support both Linux and Windows platform.
9. The IP BASED NVR shall be capable of digitally signing stored video and digitally sign exported video to ensure chain of trust.
10. The IP BASED NVR shall have failover and redundancy built in with seamless playback without manual intervention.
11. The IP BASED NVR shall support a minimum of 200 recorded video streams and 20 playback streams with minimum playback of 400 Mbps.
12. All equipment shall be modularly upgradeable so that it does not need to be replaced in its entirety to increase memory capacity, to upgrade processing performance, or to reconfigure I/O options.
13. Normal state (non-alarm) recording configuration to provide for "Detection" as defined by ULC-317-1997 and as follows:
    - Resolution HD
    - Normal Frame rate of 25 FPS
14. Alarm state recording configuration to provide for "Recognition" as defined by ULC-317-1997 and as follows:
    - Resolution of HD
    - Frame rate of 25 FPS
    - Alarm state recording of one track of audio at 32 Kbit

Technical Requirements- Central Application for CCTV Surveillance

1. The software shall be able to run on any PC based on industry standard OS.
2. The software shall support ONVIF compliant cameras and devices.
3. The software shall show live video from IP Cameras and Video Transmitters in MJPEG, MPEG4 and H.264 formats.
4. The software shall support cameras with resolutions ranging from Standard Definition, High Definition (HD) and up to 5 Megapixel.
5. The software shall show video across 4 displays per workstation - each display can have up to 25 viewing panes.
6. The software shall allow configuration of the video and audio stream settings for each user, depending on the support hardware.
7. Users shall be able to change the video pane layout in each of the 4 screens independently:
    - Grid layouts: 1x1, 2x2, 3x3, 4x4, 5x5
    - Widescreen layouts: 2x3, 3x4, 4x6
    - Hotspot layouts based on 3x3, 4x3, 4x4, 5x5 larger pane in top, left
    - Hotspot layouts based on 4x3, 4x4, 5x5 larger panes in centre
8. Users shall be able to change the aspect ratio in each of the 4 video windows independently in order to display Standard Definition or High Definition video. Choose between:
    - Widescreen (16:9)
    - Standard (4:3)
9. Users shall be able to move any image from one display screen to another via drag-and-drop.
10. Users shall be able to digitally zoom up to 1000% and also digitally scroll live video from any camera using the mouse wheel.
11. The software shall allow the removal of interlacing artefacts from 4SIF video using the following criteria:
    - Best performance
    - Best image quality
    - Smoothest rendering
12. The software shall allow the display of objects detected via analytics on the video (up to 10 at once).
13. Users shall be able to view stream statistics on all current video streams, including the following information:
    - Frame rate
    - Resolution (SIF, 2SIF, 4SIF, 720p, 1080p, 5MP)
    - Current bit-rate

- Audio bit-rate

General Technical Requirements

1. The camera shall use an Ethernet 10/100Base-TX network interface with RJ45 connector.
2. The camera and the associated equipment shall support communication protocols IPv4, IPv6, TCP, UDP, HTTP, HTTPS, DHCP, IGMP, ICMP, ARP, SNMP, Telnet, FTP, NTP, RTSP, and RTP as a minimum.
3. The camera shall incorporate a built-in web server, built-in FTP server, and a built-in FTP client.
4. The cameras shall have, at a minimum, the following configurable features:
   - Image resolution
   - Frame rate
   - Image quality adjustments (brightness and contrast)
   - Source and destination IP address settings
   - UDP port number
   - Bandwidth limits
   - Unicast and multicast settings, and
   - Support for two (2) simultaneous unicast streams
5. The cameras shall support at the minimum two individually configured video streams. The cameras shall be capable of two or more simultaneous streams with one of the streams being in H.264 format.
6. All cameras shall have an operating temperature range of 0°C to +60°C (14°F-40°F to 122°F) at humidity: 5% -95% RH.
7. The environmental housing shall be of suitable size and provide a temperature controlled atmosphere for the camera, lens and receiver driver.
8. The housing shall allow for easy disconnect of all external cables.
9. The housing, mounting arm and the dome camera installed assembly shall be suited to withstand wind gusts of 150 km/h.
10. The housing shall meet the IP67, IK10 for protection.
11. Operating Temperature for IP BASED NVR shall be 10°C to +35°C.
12. The cameras shall have a Mean Time between Failure (MTBF) of at least 150,000 hours.

4.4 Kashi Solid Waste Management System (KSWMS)

The Solid Waste Management platform proposed includes RFID's and Volume sensors installed in garbage bins to automatically monitor the status and transmit that information KICCC. The KICCC in turn should process the data and allow the Supervisors and Operators to monitor the status real time and schedule an on-demand cleanup as

recommended by VSCL. The platform should have event generation capabilities that notify the Supervisors and Zonal Officers and the Commissioner through Mobile App, when garbage bin is filled up. In addition, the SWM also allows better inventory maintenance and reduces wastage of trips of the vehicles.

The garbage sensor devices should be mounted on the top of the bin and looking in to the bin, it utilizes ultrasonic to measure the garbage level in a bin. SWM consists of three parts, the sensor web service which allows the users to view the real time status of the in each ward and receive notification on critical (both mobile and web). In addition, the application should provide a historical view of the data from all the deployed like the cleaning pattern and the timing. This will also allow us assess the efficiency of the concerned departments.

MSI has to procure and install RFID's and volume sensors. The network connectivity has to be planned and implemented to share the Smart Elements information to Command Control Center for further processing. It is Sis responsibility to procure RFID readers, Smart phones and thumb readers as mentioned in the RFP.

MSI should use the Smart elements and geo fence and geo tag them it with GIS Maps. The Vehicle/Location tracker should also be geo fenced and will be used for route optimization of garbage collecting vehicles.
Grievance application should be part of the Mobile App and the app should be Varanasi GIS Maps.

KPIs for Solid Waste Management System

1. The Smart Solid Waste Management System shall enable the level of solid waste, recycled waste, to be remotely monitored using wireless sensors installed inside the waste bin.
2. Registration/Geo-tagging and smart monitoring of all garbage bins and points.
3. RFID based system shall allow real-time tracking of waste collection system efficiency
4. Registration/Geo-tagging and smart monitoring of all Temporary Transit Station (TTS).
5. Smart mechanism for registering, monitoring and efficient and quick redressing of citizen grievances.
6. Implement a GIS/GPS enabled Solid Waste Management System to automate the entire process including online tracking of waste collection vehicles, their routes, and temporary transit stations (TTS) and attendance of public health workers.
7. Web based monitoring of each type of waste disposal separately.
8. Is solid waste collected properly from the bins?
9. Is the weight of the waste correct?
10. Tracking of solid waste with necessary checks-and-balances.
11. Process management of people, vehicles and other components involved to be monitored.

12. Daily, weekly, monthly reports on item-wise, dept. wise and activity wise details and the Consolidated Report generation on solid waste management site activity through the Command and Control Center should be made available with the real time captured data.
13. Decision support system that monitor process compliance, efficiencies and SLA monitoring shall be part of the project.

Functional Specifications for Solid Waste Management System

1. The solution shall be based on open source technology.
2. The solution recommended should comply with standards and guidelines of Govt. of India and Govt. of Uttar Pradesh.
3. The solution must have role based access and management according to the rules of VMC.
4. The solution must have the ability for logging, audit, and tracking of any changes carried out on the database. Only authorized users according to their use rights may make entries to the database.
5. The solution should support N-tier architecture
6. The solution must support Single-Sign On facility
7. The solution should support PKI based Authentication and Authorization, in accordance with IT Act 2000, using the Digital Certificates issued by the Certifying Authorities (CA).
8. The solution must maintain Interoperability Standards ensuring that the Software developed is easily integrated with the other Software
9. The architecture should be scalable (cater to increasing load of internal and external users and their transactions) and capable of delivering high performance
10. The solution must follow stringent security features such as:
    - The security services used to protect the solution shall include: Identification, Authentication, Access Control, Administration and Audit and support for industry standard protocols.
    - The solution shall support advanced user authentication mechanisms including digital certificates and biometric authentication.
    - Security design should provide for a well-designed identity management system, security of physical and digital assets, data and network security, backup and recovery and disaster recovery system.
    - The solution should provide for maintaining an audit trail of all the transactions and should also ensure the nonrepudiation of audit trail without impacting the overall performance of the system.
    - The overarching requirement is needed to comply with ISO 27001 standards of security.

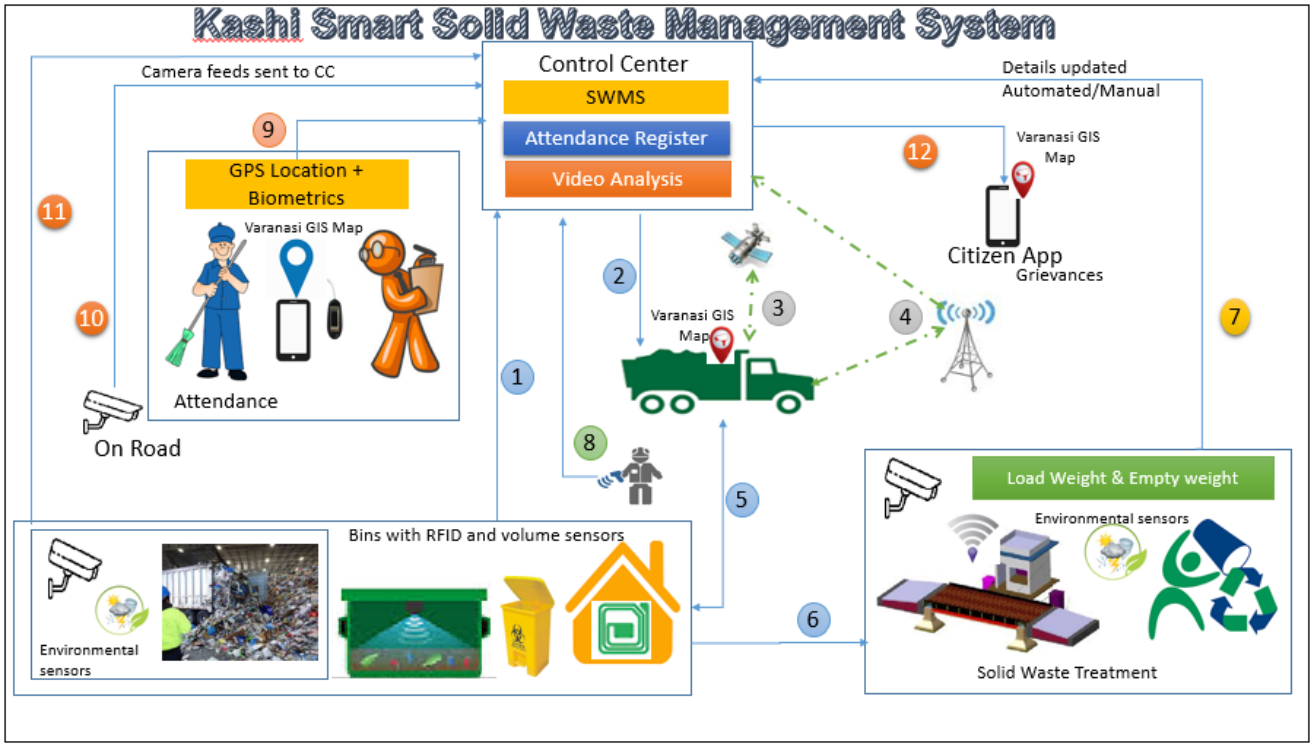


Figure : Illustrative Representation of Kashi Smart Solid Waste Management System.

11. The solution must be compliant with latest versions of Industry Standards such as W3C specifications, Information access/transfer protocols SOAP, HTTP/HTTPS, etc.
12. The required application must be made scalable and robust. It should be designed and developed in such a manner so as to allow integration with other applications in future if necessary.
13. The application should be able to integrate with SMS Gateway, Payment Gateway, Handheld PoS Devices, SMTP, RFID Tracking and Boom Barriers, CCTVs and live video streaming.
14. MSI has to get the application security audited by the CERT-IN empaneled Security Agencies.
15. MSI has to address all the compliances raised by the Security Agency and handover the security audited certificate before hosting.
16. Solution should provide GIS based interface to view all the bin points, at a glance, on location basis and bin Points locations should be integrated with digital images.
17. GIS system shall have the required layers such as Zone, Circle, Ward and Locality Temporary transit locations.
18. Design the web based GIS application denoting all the graphical locations.
19. Collect and configure the Geo-Locations as per the project requirement.
20. Design the Geo-fencing reporting portal
21. The GIS system should be web enabled and reporting should be role and right based.

22. Development of GIS system with spatial Database and integrate with the Data captured above for geographic queries and normal data queries.
23. GPS tracking of the waste pick up vehicle for real time tracking.
24. The application software should have facility to read / integrate / capture the GPS data of the vehicle.
25. Different kind of MIS report shall be generated from the application software for vehicle tracking.
26. Route Optimization which shall help in reduction of trip time, fuel saving and serving more locations.
27. Manage routes and vehicles dynamically through an automated system.
28. Efficient monitoring and management of waste collection bins.
29. Ensure complete coverage of door to door and community collections served by vehicles.
30. Monitor and track other municipal corporation vehicles under Solid Waste Management Dept.
31. Record history of vehicle routes, attended sites and other details.
32. Radio-frequency identification (RFID) devices with vehicle and RFID tagging of Bin to ensure serving by requisite vehicle.
33. Volume Sensor based bin to indicate maximum utilization status and trigger vehicle pick up.
34. Shall be integrated with Waste treatment plants to receive details of waste transit.
35. Alert / Alarm management - Real time management of missed garbage collection points.
36. Monitoring & Reporting Application - reports of vehicles, garbage collection status, bin status etc.
37. Mobile Application - Development of mobile application in open source platform for each application module is also proposed:
    - Should include Grievance redressal module and ability to capture and upload image of related complaint or grievance.
    - Should have the capability to be integrated with other mobile applications related to VMC activities.
    - App must also have the functionality to enable supervisors, transporters and other appropriate concerned officials to update the status of their activities.
    - App should send GIS location, Date**:**Time with Biometric details/Photos to control center which will be authenticated through registered mobile number of supervisors.
    - Capture images of Bin Points and transmit to the central server with text, image and GPS data such as date and time, Latitude and Longitude as per the schedule given by VMC.
    - App must enable the sending of related SMS when required.

Functional Specifications- Vehicle and Bin

1. Web Based Vehicle Tracking and Monitoring Application customized to meet the functional requirements of the solution is envisaged.

2. System shall use the Automated Vehicle Locator Management System of the Intelligent Transport Management System with customized dashboard specific to monitoring and tracking of solid waste management activities.
3. Ensure complete coverage of door to door and community collections served by vehicles.
4. The waste collection vehicles shall be fitted with RFID readers. RFID readers identify the RFID tags installed in each of the collection and house hold Bins which read the Bin details. This data shall be transferred through the GPS device unit having GSM/GPRS connectivity. RFID readers shall be integrated to the vehicle GPS device unit to achieve this functionality.
5. Varanasi map provided by the VSCL shall be used for mapping of all smart elements in the city.
6. Weight and Volume sensors 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 control centre which then shall send the information to nearest vehicle for pick-up.
7. Volume/Fill level sensors can be either Ultrasonic or IR based 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.
8. Foul smell detection sensors/ Animal repellent sensors to be installed at select locations to the garbage bin, Kooda Ghars to detect the quality of air being released into the atmosphere.
9. Surveillance/ANPR Cameras to be installed at select Kooda Ghars.
10. This system shall be integrate with the RFID system, weight and volume sensor system for bin collection management.
11. Alert / Alarm management - Real time management of missed garbage collection points.
12. Application shall be hosted in the Intelligent Command and Control Centre (ICCC). The application shall leverage on the advanced GPS and GIS technologies for route scheduling, route monitoring, reporting and providing a quick dashboard.
13. Monitoring & Reporting Application - Reports of vehicles, garbage collection status, bin status etc.
14. The platform shall have built in security for data capturing and transfer including devices used i.e. restricting to the authenticated devices only.

Functional Specifications- Transit Management System

1. System shall facilitate data transfer through GPRS enabling the update of status by the designated compactors/ tippers/ other vehicle operators on waste pick-up from bins.
2. Application must enable the monitoring of transit system of transport of Municipal Solid Waste (MSW) from designated bins at all wards to Temporary Transit Stations (TTS)/Kooda Ghars, transport of Solid Waste from designated bins to treatment centres, transport of waste from TTS to Solid Waste Treatment

Centres or any other existing/ or any other process envisaged for the future to transport waste to treatment centres.

3. Waste Treatment entry/exit stations shall be installed with RFID Readers, License Plate Image Capture Camera (ANPR, Fixed Box and PTZ) to be integrated with a local controller and workstation. If such elements/system already exist in treatment centre, System shall have the capability to be integrated with them or to receive/collect necessary data as per the VMC requirements.
4. Application must enable integration with RFID Readers, Weight/Volume Sensors and Cameras to be installed at Waste Treatment Centres.
5. Waste carrying Vehicles/Trucks shall be fixed with RFID Tags to enable their reading at the entry/exit stations of the Waste Treatment Plants.
6. System must enable the tracking of vehicles' their inward/outward movement, weight of solid waste transported to Solid Waste Treatment Centres and transfer the same to the central control centre without any ability to change the data locally.
7. All the data shall be stored locally for a min. period of 60 days including the video and images captured.
8. Application must enable integration with SMS gateway to facilitate update of status as well as notification through SMS.
9. System must enable the capturing of GIS information of the TTS and Treatment Centres by geo fencing of the same.
10. Geo tagging of all designated Bins in all wards by which the latitude and longitude details are reflected in the module pin pointing the location of the Bins. All the Bins are to be codified before geo-tagging with a facility for future scalability.
11. System must also enable the highlighting of the routes covered by the compactors/ tippers/ other vehicles involved through GIS mapping.
12. System should consider possibility of uploading of a picture/Video (taken through phone or Vehicle attached Cameras immediately after unloading the bin and cleaning the surrounding of the bin) of the unloaded waste bin to ensure that the waste from the particular bin has been lifted.

Functional Specifications- Attendance Monitoring System

1. GPS based mobile device shall enable VMC field staff to register their attendance (with date/time stamping).
2. The system shall periodically track the location of the staff through their GPS based mobile device and shall map (On Varanasi City Map provided by VSCL) it in the system with the pre-defined area coordinates.
3. Application should include the facility of handling the biographic details of all field level employees (both contractual and permanent) or should include the facility to be integrated with Aadhaar or any other system for authentication.

4. The attendance data must be captured daily either through biometric devices/special handheld devices/ Facial Attendance system or supervisor certification. The handheld devices shall be able to click photos for photo based attendance along with location and time details.
5. The device shall feed the data through GPRS/GSM network to KICCC for report generation and alerts. This attendance data should be integrated with the HR system of VMC as applicable.

Functional Specifications- SLA Monitoring System

1. The system must enable the mapping of the existing Service Level Agreement with all the involved stakeholders for the solid waste management.
2. The system should map the payment and penalty calculation as specified in the SLA.
3. Should interact with the other relevant modules to calculate correct remuneration and penalty as per the prevailing contracts.
4. System should be made configurable to enable the modification of rates of penalty and payment if needed.

Functional Specifications- Grievance Registration & Monitoring System

1. This system should facilitate the registering of grievances and complaints.
2. System should reflect the hierarchy of VMC for escalation of grievances for redressal.
3. System should have full redressal workflow management system with auto escalation of grievances as per set time period & escalation hierarchy.
4. System should be made fully configurable to set up desired levels of escalation hierarchy as well as configure the time period for escalation.
5. System must integrate with SMS gateway to enable the notification of status through SMS.
6. System must also integrate with Simple Mail Transfer Protocol (SMTP) to facilitate notifications to involved stakeholders/ parties through email.
7. System must enable the capture of the complaints of the citizens through call-centre as well as through the web-application.
8. System should generate unique compliant ID to enable tracking.
9. System should provide status update in the web-portal to enable tracking of complaint/ grievance status by the citizens.
10. System must enable the capture of images through mobile app for registration of complaints and grievances by concerned citizens.
11. System should facilitate Citizens complaints through SMS and its tracking.
12. System should generate a system based complaints reports and their status on daily basis.

Technical Specifications of Solid Waste Management System (SWMS):

Technical Specifications- RFID Reader

1. RFID Reader shall have operating frequency range of 865 MHZ to 867 MHZ.
2. The RFID reading range of the transceiver antenna mounted on the vehicle at an average height of 3m above the road surface shall be up to 5m.
3. RFID Reader antenna type shall be Circularly Polarized.
4. RFID Reader shall comply with the protocols: EPC Gen 2, ISO 18000-6C and shall comply with the general conformance requirements of the standard.
5. RFID Reader enclosure shall be light weight.
6. RFID Reader technology deployed should have the capability to optimize read rates for the bin identification application and adapt to instantaneous noise and interference level.
7. RFID Reader shall have capability of diagnostic and reporting tools.
8. The firmware should be upgradable to support future protocols.
9. Reading of Tag & EPC memory for at least 2 tags per second for a moving vehicle with a speed limit of up to 40 kilometres/ hour.
10. It shall support RF Power of minimum 0~30dBm and shall be software programmable.
11. RFID readers shall communicate over TCP/IP and GPRS or higher.
12. It shall support communication interface RS232 at minimum.
13. Readers shall be IP 65 rated.
14. RFID readers shall be capable of withstanding standard material handling vehicle environments. It shall meet or exceed MIL STD 810F.
15. Readers shall be powered by Vehicle DC Power 12 to 60V, 4.5A maximum.

Technical Specifications-RFID Tag

1. The tag shall be anti-metal, and can be mounted on the metallic surface.
2. The tag shall be high temperature resistant and shall be capable of withstanding harsh or challenging conditions.
3. The tag shall have long read and write distance.
4. The tag shall be durable, reusable.
5. The frequency range of the tag shall be between 865~867MHz.
6. The tag shall support operation mode of Fixed Frequency or FHSS Software Programmable.
7. The tag protocol shall be ISO 18000-6C & EPC CLASS1 GEN2.
8. The tag memory configuration shall be EPC: 96bit (H3) and User: 512bit (H3).

9. The tag material compatibility shall be metallic and non-metallic substrates.
10. The read range (m) on metal surface shall be max. 7.5m for Fixed Reader and max. 3m for handheld reader.
11. The Mounting of tag shall be of screw, rivet, superglue, ribbon, double faced adhesive tape type.
12. Tags shall be IP 68 rated.

Technical Specifications- Bin Volume Sensor

1. The ultrasonic bin level sensor shall be used to sense the distance from the mounting point to the bottom of the garbage bin or collection truck to measure fill levels. The sensor shall have in-built M2M communications capability for data transfer between sensor & KICCC.
2. The sensor shall sense distance of minimum 3 meters.
3. The sensor data shall be used to obtain the fill level of the waste bins.
4. The sensor shall be IP67 rating (water & dust proof) and shall be capable to operate in conditions inside waste bins. These waste bins may contain solid waste, wet waste, industrial waste, or others as per the site conditions.
5. The sensor shall be easily mountable on the waste bin.
6. The sensor shall have supporting Lithium Ion battery pack with a minimum working life of 10 years.
7. The sensor should send automatic alarm to the KICCC when the battery is about to run out of charge.

Technical Specifications- Sensor Processing Unit

1. The sensor processing unit shall be the on-board processing unit of the bin level sensors.
2. The unit shall take input from the ultra-sonic bin level sensor.
3. The unit shall process the input from level sensor (bin) into desired output format and transmit back to the central system via M2M Communications.
4. The unit shall send minimum 10 times or more (as required) data per day to the central software. This data pulling shall be user configurable.
5. The unit shall send the data to central server when the bin & waste collection truck shall be 30%, 50%, 75% and 90% filled with different level of alarms as configured by the user.
6. Once the bin & waste collection truck would be emptied, it shall send the signal to central software to confirm the same.

Technical Specifications-

Fixed Box Camera with Outdoor Housing and Lens – 2MP

Sr. No.	Description	Required Parameters
1	Image sensor	1/3" Progressive Scan CMOS or better
2	Lens	CS Mount: 5-50mm, DC-Iris, Megapixel IR corrected Lens
3	True Day and Night	Yes
4	Minimum Illumination / Light Sensitivity	Color: 0.3 lux F1.4; B/W: 0.08 lux; F:1.4 or Better
5	IR Filter	Automatic Built in IR Cut filter
6	Shutter Speed	1s to 1/30000
7	Video Compression	H.264 High, Main, Base profile and MJPEG
8	Resolutions and frame rates (H.264)	1920 x 1080
9	Video Streams	Minimum 4 @ H.264, 2MP, 25 fps or better
10	Power Supply	Power over Ethernet (PoE) IEEE 802.3af Class 2
11	Pan/Tilt/Zoom	Digital PTZ
12	Digital I/O (Alarms)	DI x 1; DO x 1
13	Local storage	SD Card Slot with 128GB Support
14	Image Settings	Color, Brightness, Sharpness, Contrast, White balance, Image Mirroring, Text and image overlay, Privacy mask, Rotation: 0°, 90°, 180°, 270°, Exposure control, Exposure zones, Fine tuning of behavior at low light, Mirror Image
15	Supported Protocol	IPv4 & v6, HTTP, HTTPS, SSL/TLS, QoS Layer 3 DiffServ, FTP, CIFS/SMB, SMTP, Bonjour, UPnP ,SNMPv1/v2c/v3(MIB-II), DNS, DynDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS, SSH
16	Security	IEEE 802.1x, IP Address Filter, Password Protection, Digest Authentication

17	ONVIF	Profile S & G
18	API	The interface shall be available for integration with 3rd party analytics and applications in public domain free of cost
19	Operating Conditions	- 10°C to 50°C, Humidity 10–100% RH (condensing)
20	Privacy Mask	Required with Minimum 2 Zones
21	Image Configuration	The camera allows include/ exclude area in any shape in order to reduce false alarms and bandwidth/ storage
22	GOV Length	It is possible to vary the GOV length in the camera setting for better control on bandwidth
23	Wide Dynamic Range	Minimum 120 dB True or Better
24	Event Triggers	Motion Detection, Edge storage events, External Input, Time Scheduled, Camera Tampering, Software alarms. The camera shall be able to send and receive trigger directly from any other camera without interface of VMS.
25	Event Actions	FTP or HTTP or network share, EMAIL, Notification via HTTP to other camera or device, Pre and post alarm video buffering, External Output Trigger, PTZ Preset, Guard Tour
26	Firmware Upgrade	The firmware upgrade shall be done though web interface, The firmware is available free of cost
27	Embedded Applications	The camera shall provide a platform allowing the upload of third party applications into the camera
28	Memory	512 MB RAM, 256 MB Flash with Support for Edge Based analytics from 3rd Party
29	Housing	IP 66 Rated IK 10 rated for outdoor use
30	Certifications	CE, FCC, IEC, EN, UL
31	Warranty	5 years OEM warranty

4.5 Kashi Environmental Monitoring System (KEMS)

Environmental pollution, particularly of the air, is nowadays a major problem that unknowingly affects lives in the cities. As clear focus of building [city] as one of the finest example of SMART city, Authority believes it is important that citizens know of the air that they breathe. Citizens & visitors to City can enjoy unique experiences that keep them feeling good by knowing city's environment condition at different locations.

The Air quality should be monitored by a network comprising:

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

KPIs for Environmental Monitoring System:

- Provide better quality air to citizens of Varanasi
- Monitor environment pollution and have measures to control pollution
- Environmental monitoring to be implemented in all major parts of the city especially in crowded places
- Environmental monitoring should consist of measuring levels for Temperature, Humidity, Ambient Light, Sound, Pressure, CO, CO2, NO2, O2, SO2 and compulsorily PM 2.5 and PM 10.
- Integrate with other disaster management applications from other nodal organizations of environment
- Additional monitoring will be done in crowded areas of Kashi
- Environment monitoring sensors will be installed dump yards and solid waste management locations and crowded areas of Varanasi

The MSI should:

- Install environment sensors (as per the functional requirement) & display environment related information at various strategic locations through variable message system
- The environment sensors shall be integrated with the central control system at KICCC to capture and display/ provide feed on Temperature, Humidity, Pollutants like SoX, NoX, CoX, etc, Noise Pollution, Electromagnetic Radiation, UV radiation etc. The data collected should be location-marked.

- 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.
- Then this information is relayed instantaneously to signage – large, clear, digital-display screens which let citizens know regarding the prevalent environmental conditions. The environmental monitoring data should be displayed by picking data from VMS application in real time.
- Further environmental sensors recorded data shall be used by Mobile application developed as part of e-Governance to enable user for alarm management and notification of environmental details on real time basis.
- Grievance Redressal of Citizen integration to e-Governance Mobile App 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.

Components of Environmental Sensors:

1. Wireless Environment 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

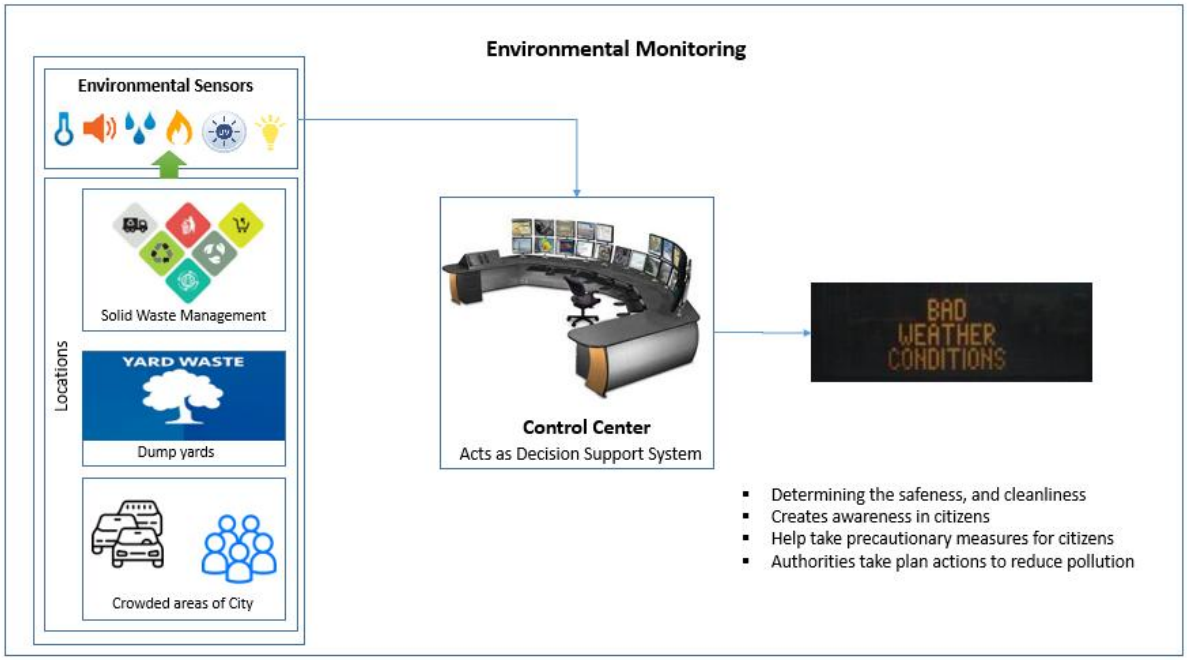
4. Variable Message Board

    - Shall receive information from the central application System and operate accordingly

Functional Specifications for Environmental Monitoring System:

1. Smart environment sensors should gather data about pollution, ambient conditions (temperature and humidity), levels of gases in the city (pollution) and any other events on an hourly and subsequently daily basis. User should be able to set the schedules as per requirements. It is for information of citizens and administration to further take appropriate actions during the daily course / cause of any event.
2. The environment sensors should be having the following capabilities:
    - They should be ruggedized enough to be deployed in open air areas, on streets and parks
    - They should be able to read and report at least the following parameters: Temperature, Humidity, Ambient Light, Sound, Pressure, CO, CO2, NO2, O3, SO2 and compulsorily PM 2.5 and PM 10 Noise and UV
3. The analysers must function properly in all conditions without any defect between 0 to 50 degrees C ambient temperatures, 0 ambient dust levels. The data capture rate should not be less than 90%
4. The manufacturer of the Equipment should assure technical support for the equipment for the duration as indicated in the scope
5. Smart environment sensors will inform and enable citizens and administrators 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 or Wi-Fi networks. It is not mandatory to connect all sensors via MPLS fiber network.
6. 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. It is preferred if the platform also includes intelligent analytical engines that makes information meaningful to all stakeholders and helps ease decision making.
7. Integration of environmental monitoring system with Variable messaging system to be displayed wherever possible (need to be finalized post detailed survey of locations).
8. The sensor management platform should allow the configuration of the sensor to the network and also location details etc.

9. The sensors should be able to be managed and calibrated remotely. This includes sensors being updated with calibration parameters, software upgrades. Sensors must also provide updates and detect faults with self-diagnosis functionality.
10. Apart from information provision, the sensors must ensure data is transmitted securely and have security measures from sensors to the software platform. It must also ensure tamper alerts are provided in cases of vandalism, security breaches, etc.
11. Any sensor failure should alarm and generate an event that should be linked with Incident Management system automatically and should be capable to schedule the automation of sending the failure report to the vendor
12. The sensors provided should to 99% accurate and should of industry standards
13. Apart from information provision, the sensors must ensure data is transmitted securely and have security measures from sensors to the software platform. It must also ensure tamper alerts are provided in cases of vandalism, security breaches, etc.
14. Calibration system should be provided for the calibration of the air quality analysers, data acquisition system.
15. The data collected should also be available on permitted mobile devices as necessary
16. Real time or averaged data can be viewed quickly and easily client interface on the central computer
17. It should have a feature for viewing instantaneous and historical data in the form of tables and graphs either locally or from a remote client
18. Generation of reports for pollution load, wind etc should be available
19. Alarm annunciation of analyzer/sensor in abnormal conditions in the control center so that appropriate action can be taken by authorities
20. The environmental sensors should be visible as a layer in GIS Maps



Technical Specifications:

S No.	Parameter	Specification
1	**Measurement elements**	Temperature, Humidity, Ambient Light, Sound, CO, NO2, O3, SO2, PM2.5, PM 10
2	**Measurement component Measurement range**	O3 : 0 – 390 ppb
		SO2 : 0 – 630 ppb
		CO : 0 – 31 ppm
		CO2 : 0 to 10% / 0 to 20%
		O2 : 0 to 10% / 0 to 25% (2 ranges each, maximum range ratio 1: 25 except O2) *Optionally, N2O and CH4 can be measured
		PM 2.5: 0 to 250 micro gms / cu.m
		PM 10: 0 to 450 micro gms / cu.m
		Light: up to 10,000 Lux
		UV: Proportion of UV Present in µW/Lumen & Total amount in µW/M2
		Noise: up to 100 dB (A)
3	**Temperature, Pressure and Humidity Sensor**	Real-time Temperature Range: outdoor 0ºC ~ 50ºC
		Real-time in Air Humidity Level Display
		Real-Time Pressure Display (in Bars or millibars)
4	**Connectivity**	Wi-Fi, Ethernet or GSM (3G)

		Sensors must have provision to interchange between Wi-Fi or GSM systems easily
5	**Software and Data backup**	Backup measurement data for up-to 5 days in case of network failure or system maintenance cycles
6	**Mechanical Enclosure**	Single enclosure with all components inside or simplified mounting
7	**Data validity and stabilization**	Sensors must ensure data of sensors is valid and not require stabilization times in case of power outages less than 5 hours.
8	**Product origin and certification**	Must also qualify a minimum international standards on product certification such as CE, FCC and PTCRB
9	**Rain Water measurement**	in mm
10	**Repeatability**	±0.5% FS
11	**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
12	**Respond Speed**	120 seconds max. for 90% response from the analyzes inlet

4.6 Kashi Smart Parking Management System (KSPMS)

Varanasi Police covers an area of about 112.26 Sq. km. The following map represents the Geographical spread of the area and zone wise distribution of police jurisdictions. This includes Varanasi Municipal Corporation limits.

Residents of Varanasi are facing trouble in finding parking space and frequently end up in wrong parking practices. The Smart Parking solution will alert residents about parking spaces available, allow them to pay with mobile wallets or bank wallets or mobile wallets like payTM etc through their mobile phones.

Varanasi being a religious and cultural tourist place there are over 70,00,000 pilgrims visiting the place. Therefore, number of floating vehicles enter into the city on daily basis apart from local vehicles. VSCL has identified 9 locations in the city for parking. Out of which there will be one dedicated multi-level parking for two wheelers and one multi-level car parking which will be completed on priority basis.

Challenges with Conventional Parking:

1. High Parking Search Time
2. Traffic Congestion on Road
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
Increase quality of life	▪ Simplifies Payment
Improvement in citizen's parking experience & satisfaction	▪ Easily finds the parking space
More efficient use of parking	▪ Time saving
Reduces illegal parking	▪ Avoid traffic congestion
Reduces revenue leakages	
Reduces Man power cost	

Smart Parking – Mobile Solution & its Benefits (Subset of Smart Kashi Mobile App and Smart Kashi Portal):

1. Mobile App for 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. Availability of data & Analysis for growing need for expansion or more parking slots; subsequently required measures to handle problem

General Requirements

1. Installation of sensors in each bay, which register whether the bay is occupied or vacant.
2. Installation & Maintenance of Variable Message Boards in the parking
3. Integration with VMS which is managed from Integrated Command Control Center
4. Network and backup mechanisms for power
5. Installation and boom barriers and cameras
6. The Mobile ticketing devices required for payments and integrated with Parking Management Application
7. Fully functional Parking Management System as specified in FRS
8. This information to relay live to local and Central system where parking management application is hosted, which collates and analyses the data.
9. Mobile App feature to view, book the parking space as mentioned in functional and technical requirements.
10. Smart elements geo tagging with GIS Maps and all the operations from command control center should use GIS Maps as interface
11. Mobile App should use Varanasi GIS Maps
12. Payment gateway integration

KPIs for Smart Parking:

1. Reduce parking sear time for citizens and pilgrims visiting the city

2. Reduce traffic congestion caused by people searching for parking space
3. Optimize parking lot usage by appropriate planning and restructuring
4. Add smart elements for parking spaces to manage vehicles
5. Identify open spaces and on road parking options
6. Increase revenue collection through managed parking
7. Improve parking experience to vehicle owners
8. Reduce greenhouse gases by decreasing search time for parking spaces
9. Monitor vehicles entering parking lots
10. Provide real time tracking of parking availability on mobile and VMS
11. Online or wallet payments through mobile device to ease transactions
12. Gather data for analytics and planning

Functional Requirements of Smart Parking Management System (SPMS):

The following requirements are meant for multilevel 2 wheeler and multilevel car parking. Additional requirements of the parking system for multilevel car parking is called out in the last section of smart parking functional requirements.

1. The Kashi Smart Parking Management System (KSPMS) should enable VSCL to obtain real time situational awareness about the occupancy of parking lot.
2. The KSPMS should enable VSCL or any other appointed third party to manage parking locations
3. The smart parking solution should provide real time location based view to citizens about proximity of parking lots and availability of parking lots
4. The smart parking solution should enable the above functions with minimum manual intervention. The smart parking solution is envisaged for closed parking lots, open parking lots and road side parking as implemented as applicable
    i. **Multi-Level Parking Spaces**- Such parking spaces are managed by VSCL through sub contracted vendors initially and the parking lots have boundary walls and a defined entry and exit points. Parking spaces have specified number of slots available at each floor for two wheelers and four wheelers as required.
        ii. **Open Parking Spaces**- Such locations are managed by VSCL through sub contracted vendors and have a boundary wall and defined entry and exit points. These kind of parking spaces have specified number of slots available, typically in an open ground or road.
        iii. **Road side parking spaces** - These locations will be identified by traffic police at various locations of the city. These identified parking areas will have clear demarcations for parking and required sign boards. These will be managed sub-contractors.
5. Configurable with multiple parking locations and available number of slots for each locations

6. The smart parking solution should be able count the number of vehicles entering and exiting any parking structure except parking on road sides
7. The smart parking solution must geo-reference all the parking lots.
8. The smart parking solution will use video camera based analytics for parking lots without sensors (Open parking) and two wheeler parking and sensor based solutions to determine number of vehicles entering and exiting parking lots for multi-level parking. The smart parking solution should do so at each floor, in case of multilevel parking and communicate the data
9. The smart parking solution should report occupancy of parking lots to a central software application deployed at the command center using the network laid out as a part of this tender document
10. For Multi-level car parking the parking slots will be identified with unique ID and can be booked from internet or mobile device
11. Application should be able to manage third party contractor details
12. Real time display of parking slots availability for each location should be available on Mobile App and on web page
13. Receive & Send parking details to Mobile App
14. Receive & Send details to parking location wireless devices including Mobile App bookings and display units
15. The parking block time for Mobile App user should be configurable from Server and displayed in Mobile App
16. Application should be able to configure time allowed to extend for blocked parking and the same will be displayed on Mobile Apps like: He can extend time by 5 minutes if he is nearby so that the blocked parking will be released after 5 minutes for only multi-level car parking
17. The bookings received from the Mobile App should be updated at the control center and also at the parking location displays
18. The availability of parking slot should be displayed on Variable Message System (VMS) from control center and not through Mobile ticketing device
19. The total number of slots and free slots for parking must be displayed on a digital signboard near the entrance of the parking lots or as specified by VSCL.
20. The smart parking solution should facilitate real time revision of parking fees and should enable real time communication of rules to handheld terminal and parking kiosks. A sign board should be displayed in entry gate to notify the user regarding demand based parking fee
21. Save information in SQL or equivalent database
22. Reporting & Analytics - The smart parking solution should enable accounting and mapping of individual parking spots.
23. Audit trials of open loops for car parking should be automatically displayed on dashboard

Functional Specification of Wireless Handheld Devices:

1. Receive available parking information from control center
2. Allocate parking space to local users and generate ticket
3. Generate ticket of the mobile users via QR code reading from mobile devices
4. Update control central web-server with allocation information
5. Integrated with local display unit for parking status information and boom barrier operations for which logs to be created in KSPMS
6. Similar device at the exit location should work as payment collection device or same device if enter and exit are next to each other
7. The calculated amount will be received from Smart Parking Application
8. In case of failure of network, the amount should be calculated manually and same should be updated to KSPMS later

Functional Specification of Wireless Handheld Device Modes

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 fall back mechanism. However, this device must track every transaction limiting any manual transaction to zero.

i. Street Parking Mode:
   - It should be possible to use wireless handheld devices in street parking model
   - On arrival of motorist, it should be able to dispense a ticket
   - The same device should also be able to function as cash register
   - The transactions should get uploaded instantly and automatically to the Kashi Smart Parking Management System using online connectivity.

ii. Indoor or Open Parking Mode:

iii. 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.

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

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

vi. 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.

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

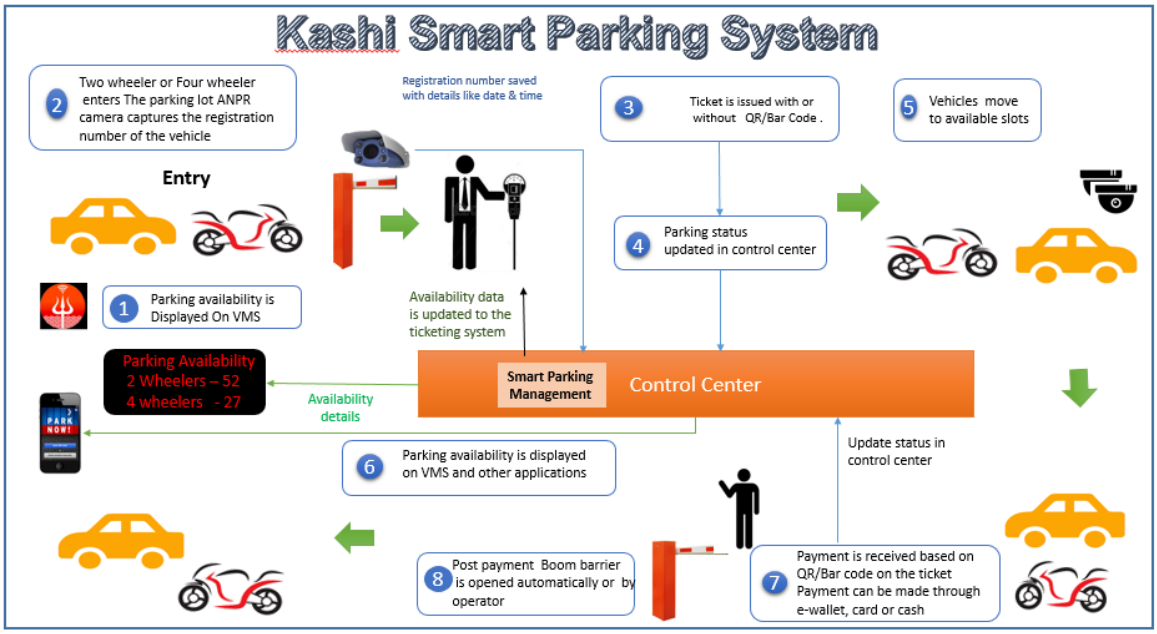


Figure : Illustrative Representation of Kashi Smart Parking System.

Functional Specification of Mobile App

1. The smart parking solution should have a mobile and a web delivery channel for citizens to get real time parking availability
2. A mobile application (sub section of VSCL umbrella application to be developed as a part of this tender) and web based user interface (application to be made available across all leading platforms) should be provided with the following features:
3. The application should have citizen module and officer module for police.
4. Through the citizen module, the user should be able to locate nearest parking lot on his geographical coordinates. The same information must be made available on map with routing information.
5. The citizen should be able to see all the parking lots with exact available space in a real time mode.
6. While locating nearest parking lot, the latest parking slot availability should be given to the user.
7. The application should have a compliance officer module where VSCL designated inspector or operator will be able to check compliance of slot occupancy against the fees paid by the citizen and

the mobile will vibrate or alarm the pole nearby police about the fully occupied parking so that he can divert the traffic and also command control can send details nearby parking locations

8. The citizens should be able to generate MIS report to view occupancy of parking lots over a defined time period.
9. The administrators should be able to generate MIS report to view occupancy, collection and other usage statistics over a defined time period.
10. Mobile App will connect to central web-server
11. Receive parking availability information for all the parking areas of Varanasi and by default display the availability of parking space for the nearest parking location for the citizen and officer module
12. User should be able to book a slot and receives QR code generated for the parking location
13. If the user does not arrive at the parking location at specified time, user can request to increase the block time for him which will be configured from control center
14. The QR code generated should be viewable and identified by the mobile device at the payment location of the parking
15. The extension of parking slot reaching time should be displayed with QR code with time stamp
16. User should be able to make the payment through cash or e-Wallet at the parking location
17. Mobile App will beep if the block time for parking is nearing 3 minutes
18. For only multi-level parking, user should be able to book a parking spot as configured by KSPMS.
19. All connected mobiles will request refresh internal should be 1 minute
20. All the functionalities mentioned above should be displayed on a web page. This page will be linked with existing Varanasi web site

Functional Specification of Boom Barrier & Variable Message Boards:

The units shall receive information from the Smart Parking Application and operate accordingly
The standards for above should :

1. 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
2. Be of leading industry standards and /or as per standards mentioned

Functional Specification of Entry Requirement

1. Entry to any parking space should have outdoor displays/screens showing overall availability of parking slots in the parking space.
2. Each entry and exit lane should be equipped with one Entry Device with the following capabilities:

- The Entry Device should act as an Automatic Ticket Dispenser
- The Entry Device should have Near Field Communication (NFC) capability
- The Entry Device should have capability to connect with Intercom, Microphone, Speaker and other Subsystems

3. The ticket, Bar code, QR Code (Preferred) and Smart Parking Card or any other technology used by MSI should be capable of capturing data that is easily retrievable at the exit.
4. 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.
5. 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.
6. The Entry Device should be able to detect and report:
    - Anti-pass back
    - Back-out ticket
    - c) Low ticket stock
7. The display on Entry Device should have capability to display messages in English, Hindi and other Regional languages.

Functional Specification of ANPR & Surveillance Cameras

1. ANPR camera will capture the vehicle registration number with details like parking lot number, Date & Time stamp of entry, Date & Time stamp of exit
2. ANPR camera should be capable of reading any type of number plates and may use OCR for recognition
3. The Camera should recognize other language numbers may be based on the font installation
4. ANPR cameras to be installed in all parking locations. The vehicle numbers will be sent to command control center with details like Parking lot ID, Date and Time, Type of vehicle (More details if required)
5. For multi-level car parking 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 city operation Centre.
6. For multi-level car parking the system checks daily whether the vehicles that have entered the premises but are yet to leave. Thereby KSPMS can generate alert if any vehicle is overstaying in the parking lot over 24 hrs

7. MSI can install appropriate surveillance cameras at entry and exit points, camera in each floor of multi-level car parking. The smart parking solution should retain videos of car entering /exiting the parking zone as per the security parameters defined.

Entry and Exit Barrier

1. The entrance and exit of each parking lot should have a barrier gate system using technologies such as boom barriers, bollards (Stainless Steel) etc.
2. The barrier should remain in open position for optimal period of time for the vehicle to pass at entrance and exit.
3. Barrier should have capability of in built glowing direction signage
4. Barrier Arms should have the following options:
    - In closed position the full arm should be illuminated red.
    - During movement the full arm should be illuminated yellow
    - Once reached open position the full arm should be illuminated Green
5. 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.
6. 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.
7. All vehicular passages during the time 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.
8. 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.
9. The barrier arm should be easy to refit with barrier unit in a short duration (within one minute).
10. 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 Kashi Smart Parking Management System.

Exit Requirements

1. Any vehicle, before leaving the parking area, should be stopped by a barrier system at the point of exit from the parking.
2. The solution should have clearly instructed easy to use interface
3. Should have a Manual Pay Station:

- Exit of every parking should be equipped with a manned Pay station (booth).
- The exit booth should have appropriate space for keeping devices such as a computer with internet connectivity, Bar code, QR code reader, credit card reader, printer etc.
- The payment for parking should be collected based on entry time stamp by any personnel stationed at the Pay Station.
- The fee for all the parking locations will be regulated by VSCL or sub-contractor. The fee structure for the parking lots will be managed by Smart Parking Application in control center and received in real time
- 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.

4. Once the vehicle exits a parking slot, the total parking slots available in that parking space should automatically get updated.
5. 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.
6. The solution should be equipped with Anti-pass back technology and be able to detect and report any instance pass back.
7. 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.
8. The solution should track each and every revenue source and should ensure no leakages due to manual intervention.
9. x. All type of payments modes should be possible

Parking aisle light indicators:

1. Light indicators should be installed for all indoor parking lots for motorist to see the available and occupied spaces from the parking lane easily
2. Once a parking spot is occupied the total parking slots should automatically get updated.
3. 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.
4. The MSI may suggest any similar innovative solution for Open Parking and Street Parking.

Payment options

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

2. For bookings through Mobile App or Smart Web Portal Application, payment will be made using e-Wallet, Net banking, Credit card, Debit card etc.
3. Additionally, the MSI can implement innovative and cost effective payment methods (such as e-vouchers).

Informative Display Panels

1. 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.
2. 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).

Real-time Monitoring and Dynamic MIS Reporting

1. The system should include central reporting system establishing the connection between the devices and sensors, and the centralized Command and Control Centre.
2. The solution should include reporting dashboards with location specific thresholds to be set for generating customized reports
3. The solution should be capable of monitoring the number of vehicles that entered or exited the parking premises during any given time
4. 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.
5. These reports should be available in all standard acceptable formats like .csv, .pdf, .txt, etc.

Additional Requirement for Multi-level car parking only

1. Additionally, in the above illustrative diagram, Sensors for vehicle detection will be installed at each slot in the parking lot and movement of vehicles will be monitored and managed accordingly. These sensors do not exist for open parking and multi-level 2 wheeler parking
2. The sensor should be intelligent and accurately detect if the car space is vacant or occupied.
3. 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 MSI can propose innovative, advanced but reliable implementation approaches using other sensors.
4. The sensor should be able to detect a vehicle irrespective of the depth or height of sensor installation.

5. Each sensor should have its own unique identification in order to be accurately tracked by the Parking Guidance System.
6. Each sensor should have an accurate and real time feedback mechanism to be detected automatically by the system in case of faults.
7. It should be placed appropriately per parking spot ideally fixed towards roof

Technical Specifications: Smart Parking Solution

The following standards and specification need to be followed:

1. Entry Device
    - Should be able to generate printed receipts in designated format on selecting the duration of parking
    - Conform ISO 9001 Quality Assurance Standard
    - CE, FCC, IC, CNRTLUS certified
2. Exit Device
    - Conform ISO 9001 Quality Assurance Standard
3. Entry / Exit Barrier
    - The Barrier unit must conform to ISO 9001 Quality Assurance Standard
    - CE, Ukr – Sepcro certified
    - Degree of Protection: IP34D
    - Bling lights for entry and exit
4. Display devices
    - Should display double line dynamic display with 24*24 matrix (12 digits) with a minimum size of 1000 mm * 150 mm

4.7 Kashi Smart Street Light Management System (KSSLMS)

The City has about 36077 streetlights installed on poles. All the city lights are changed to LED lights. 10,000 streetlights out of the mentioned lights particularly belongs to the ABD and nearby areas to be converted to Smart LED streetlights/ floodlights. In case the city has already installed Smart LED Street Lights within the identified streetlights, these lights to be integrated with intended Central Management server. The project that is being implemented is limited features to manage the LED lights.

Currently, existing street light system is facing issues like

1. Lack of information about the real time status of the street lights and area at a central location
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 & replacement, dimming, Alternate light ON/OFF 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
8. Issues related to smart poles

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
9. Poles functionality

General requirements

1. MSI has to replace 10000 lights with LEDs as per functional and technical requirements specified.
2. Replace the lights and maintain for the period of 5 years
3. Ensure connectivity from all the smart light locations to KICCC
4. MSI has to ensure the Smart Light elements to be geo tagged and GIS maps to be used as the operations for day to day activities and reports. In the backend the GIS Map should get the real time data from Smart Light Central Management Application.

5. All the role based operations has to be performed using the GIS Maps.

KPIs for Smart Lighting Management System

1. Reduce energy consumption, cost, and its maintenance
2. Enhance situational awareness, real-time collaboration, and decision making across city
3. Add intelligent IT innovations to civic utilities, public safety without adding significantly more physical infrastructure
4. Real-time data communications with low latency (or minimal delay), to improve safety and security
5. Real time tracking and management of street lights
6. Automatic status updates or failure alerts to remote server
7. Save energy through Lux control
8. Measure and analyze the data gathered through the smart elements and save energy
9. Smart Lights will be installed initially 5 wards
10. Existing LED lights may be replayed based on technical analysis for the selected areas of Smart Lighting
11. Existing poles will not be replaced

Functional requirements

1. Individual switch on/off, increase/decrease luminosity as per ground situation
2. Policy based Operations- 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
3. Advanced scheduling calendar using Light Control Unit (LCU) to switch on-off the individual street light using the last received scheduling information to keep the system working even if the network breaks down.
4. Measure the power consumed by the light and detect power theft.
5. Detect accidents / damage to the pole using motion sensors
6. Monitor voltage, current, voltage fluctuation, power consumption for each individual light as well as a group of lights
7. Real time status of the Smart Lighting System on a city map view of Lighting Operations Management software and GIS Map
8. Automatically switch on /off on the basis of lux level. There should be a manual override for lux level and it should be monitored when used

9. Lux levels along with additional components 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.)
10. Predefined exceptions to the lighting schedule and manual override
11. LED and grid monitoring, real-time alerts, malfunctions management and triggered commands
12. Flexible map based visualization - public or private map provider integration: ArcGIS, ESRI GIS, Google maps, Open Street maps etc.
13. Advanced user management: privilege, area allocation and system management (including independent sub-systems)
14. Advanced data analytics, reporting tools and performance graphs, featuring detailed filtering capabilities (lamp runtime reports, energy savings reports, luminary status reports, etc.)
15. Vendor agnostic, compatible with different LEDs and LED controllers
16. Plug and play for any additional devices with power and network media and protocol support
17. Multi-language interface
18. Network connectivity for street light poles, controllers and city operation center.
19. Provide Secure bidirectional communication channel that is reliable and cheaper top install and operate
20. Map based user management for better operations management
21. Should have Smart Controllers for smart lights
22. Unlimited numbers of lamp layers and lamp grouping possibilities, advanced filtering and bulk updating actions

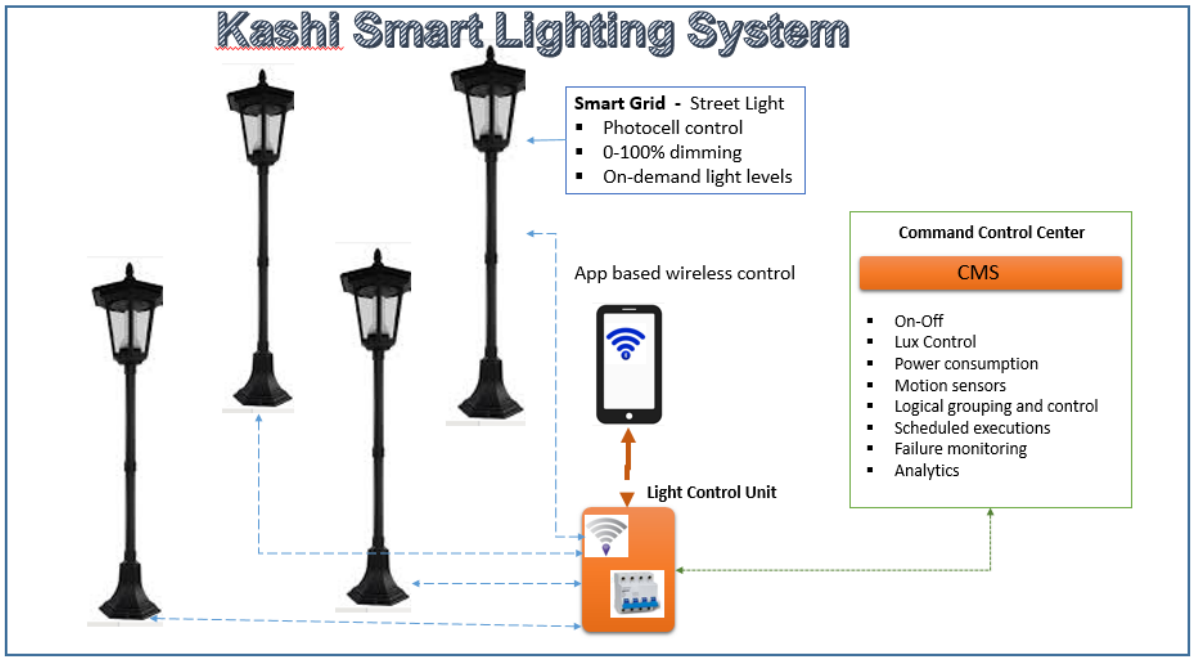


Figure : Illustrative Representation of Kashi Smart Lighting System.

23. One-time license solution that support at least 50,000 smart lights
24. Smartphone application support for installation and commissioning which can also be used during maintenance Ex: For any maintenance work the electrician should not be dependent on control center
25. Learn the existing occupancy pattern and predict occupancy patterns for future planning
26. Communication technology used should be reliable, cost effective and scalable
27. Support for other internet of things interactions
28. The application will have APIs to integrate with any existing application with electricity board
29. The data available at the control center should be accessible through web
30. There should be information about the amount of natural lux levels and that created by the street lights on a 24 X 7 basis.
31. Learn occupancy pattern and predict the occupancy patterns for future planning

Technical Specifications

A. Smart LED Lights

Supply of LED streetlight luminaire complete with pressure die cast/extruded aluminum housing and adhering to the following specifications and lighting design requirements will be as per the actual application:

- The driver card shall cut off at 270V and shall resume normal working when nominal voltage is applied again. This is to ensure protection of luminaires from neutral faults and error in connection at sites.
- Efficiency of driver electronics shall be more than 85%.
- The LEDs should be driven at the suitable current and within the permissible limits specified by the LED chip/lamp manufacturer.
- The fixture shall be designed so as to have lumen maintenance of at least 70% at the end of 50,000 hours.
- The luminaire should be operable with auto adjustable 100-270V supply Voltage using the same driver.
- Power Factor of the electronic driver should be at least > 0.95 with THD < 10%. RFP for Selection of Concessionaire for Implementation of Intelligent Street pole in Indore under PPP Indore Smart City Development Ltd. Page 214

- The luminaire should throw the perfect amount of uniform light with exactly the desired intensity, and offer best pole spacing, along with better light control. For this purpose, spacing to height ratio calculations must be attached for all installations were the poles are to be newly installed. The Luminaire shall employ individual optical lens for the each of the LED to ensure better uniformity of light distribution.

1. Key Specifications

S.No.	Electrical Specifications	25W-45W	60W-90W	100W-250W
i.	Voltage range or rating: [130 volt – 270 volt AC] on Single Phase	100-270 V	100-270V	100-270V
ii.	LED fixture Output (lumen per watt)	>110(+5%)	>110(+5%)	>110(+5%)
iii.	Frequency range (+/-5)	50Hz	50Hz	50Hz
iv.	Power factor	>/=0.95	>/=0.95	>/=0.95
v.	Color Temperature	5000K-6000K	5000K-6000K	5000K-6000K
vi.	CRI (Color Rendering Index)	>=70	>=70	>=70
vii.	LED Life Expectancy	50,000 hrs with 70% Lumens	50,000 hrs with 70% Lumens	50,000 hrs with 70% Lumens
viii.	Protection Level	IP66 Minimum	IP66 Minimum	IP66 Minimum
ix.	Total Harmonic Distortion (THD)	<10%	<10%	<10%
x.	IK rating	>/=IK 05	>/=IK 05	>/=IK 05
xi.	Surge Protection	Internal 3KV & External 10 KV	Internal 3KV & External 10 KV	Internal 3KV & External 10 KV

2. Certification CE

- Metering: EN 61326-1 (Electrical
- Safety: EN 60950-1
- Lighting: EN 61000
- EMC: ETSI EN 301 489-3

- Radio & RF Spectrum Efficiency: ETSI EN 300 220-1
- RoHS
- R&TTE 1999/5/EC
- Applicable FCC Title 47 part 15 classes
- The wireless transmission system needs to comply with the European maximum transmission power of 10mW (+10dBm) or 500mW (+27dBm), and a receive sensibility of -110dBm IP 55 (integrated controller, IP68 for external enclosure) and RoHS approved.
- The system needs to be based on the IETF open standard

3. **Power:** 110-256 VAC 50/60Hz.
4. **Optional backup power for external mounting:** NiMh 600mAh battery (with an average 10 years expected life).
5. **Intellectual Property:** The Bidder's technology needs to own 100% of the solution's IP
6. **Low power consumption:** The Luminaire Controller should consume less than 2watts.

7. **Integrated in the fixture:** The Luminaire Controller should be Internal mounting in the fixture. Node dimensions (Max) 110 x 77 x 36 mm (for internal mounting).
8. **For the non-integrated option for ad-hoc basis.** Dimensions (Max) would then be: 150 x 108 x 55 mm. Operating temperature: -30°C to +70°C.
9. The antenna could be integrated in the fixture (which would reduce the transmission/reception power) or external (TNC/SMA or via an RF coax cable)
10. **Autonomous clock:** The Luminaire Controller must store scheduled ON, OFF and steeples dimming command that it received from the Central Management Software and execute them with the light point
11. The Luminaire Controller should have an astronomical clock to define lighting schedules based on seasons. Those schedules could be defined from relative and absolute commands.
12. The Luminaire Controller should manage the luminaire even in case of a network outage (i.e. the stored lighting schedule should apply even if the controller can't communicate with the Central Management System)
13. **Control of the luminaire and Manual override:** The Luminaire Controller must be able to receive and execute real time ON/OFF (via mechanical 8A relay) and steeples dimming commands that it receives from the Central Management Software. The controller's schedule table should support up to 16 programmable commands, in an integrated non-volatile method. A local override port on the controller should be available for future use."
14. Any type of Dimming is not allowed.

15. **Communicate using a wireless mesh protocol:** The Luminaire Controllers must communicate using a wireless mesh protocol. This protocol should be open, based on the 6LoWPAN standard (802.15.4), with an IPv6 addressing scheme, on the ISM band (433MHz, 868MHz and 915MHz) or any other free band Essential"
16. **Broadcast communication:** The wireless mesh protocol shall support broadcast (one command to target a group of Luminaire Controllers) and unicast (one command sent to a single Luminaire Controller).
17. **Integrated in a Smart City environment:** The Luminaire Controllers must integrated seamlessly in identified Smart City network.
18. **Detect and report failures:** The Luminaire Controllers must be able to detect and report alarms such as: lamp failures, ballast failure, low/high voltage, low/high current, low capacitor, flickering lamps, etc.
19. **Measuring electrical values:** The Luminaire Controllers must be able to measure mains voltage (RMS - Root Mean square), current (RMS), frequency, power factor, active and reactive power, active and reactive energy; in real-time or not, with an accuracy equal or better than 2%.Integrated temperature meter. The load's electrical consumption measurement is up to 1,5kVA
20. **Measure cumulated energy consumption:** The Luminaire Controller must measure and store the cumulated energy consumption
21. **Measure number of burning hours:** The Luminaire Controllers must measure and store the number of lamp burning hours
22. **Additional I/O port for future use:** The Luminaire Controllers must have at least 2 local I/O programmable ports for future use

B. Data Communication Unit (DCU)

1. General Certification CE
    - Metering: EN 61326-1
    - Health: EN 50385
    - Safety: EN 60950-1
    - Lighting: EN 61000
    - EMC EN 301 489-1, ETSI EN 301 489-3, ETSI EN 301 489-17
    - Radio & RF Spectrum Efficiency: ETSI EN 300 220-2 v2.3.1, ETSI EN 300 328, ETSI EN 301 893
    - RoHS

- R&TTE 1999/5/EC
- Applicable FCC Title 47 part 15 classes

2. The narrowband wireless transmission system needs to comply with the European maximum transmission power of 10mW (+10dBm) or 500mW (+27dBm) and a receive sensibility of 98dBm (for the 6LoWPAN 802.15.4 communication standard), as well as 500mW (+27dBm) and a receive sensibility of -119/-115/-107 dBm (for the EN 13757-4 – Wireless M-Bus).
3. The broadband Wi-Fi transmission system needs to comply with the Wi-Fi power transmissions standards: 200mW (+23dBm) – 802.11 a/n/s and 100mW (+20dBm) – 802.11 b/g
4. The system needs to be based on the IETF open standard. IP 40 (integrated gateway) or IP67 (for external enclosure) and RoHS approved"
5. Power: 85-256 VAC 50/60Hz.12/24 DC. POE – IEEE 802.3at – 48VDC. Power consumption: 5W max.
6. Number of LED Lights to be considered: 250W &150W. Total number of poles for housing LED lights will be determines based on analysis
7. "Environmental Dimension: 269 x 239 x 82 mm (rugged metal case) or 330 x 204 x 55 mm (anodized metal case)
8. Operating temperature: -30°C to +60°C. Case:
    - External mounting: IP 67, rugged metal, resistant to oils/greases/fuels, diesel, paraffin/ozone and RoHS approved.
    - Internal mounting: IP40 anodized metal.
9. Wireless fully meshed communication protocol The gateway should be able to communicate in broadband and narrow band networks:
    - Narrowband networks (IPv6): The open standard 6LoWPAN (802.15.4) IPv6 should be supported on the ISM frequency band (433MHz, 868 MHz and 915MHz).
    - Broadband network (IPv4): The following standards should be supported:
        - Wi-Fi 802.11 a/b/g/n/s standard on the 2.4GHz, 5.4GHz or 5.8GHz frequency bands
        - GSM/GPRS/EDGE/UMTS/3G on the 850/900/1800/1900 MHz frequency bands
        - RJ-45 10/100Mb base-TX Ethernet port
10. The gateway needs to communicate and route traffic between the different networks automatically and in real-time.
11. Communication performance
    - Narrowband network: The fully meshed wireless network should support a bandwidth of up to 200Kbps
    - Broadband network: The fully meshed wireless network should support a bandwidth of up to 300Mbps"

12. Broadcast communication: The wireless mesh protocol shall support broadcast (one command to target a group of Controllers/Nodes) and unicast (one command sent to a single Controller/Nodes)
13. Integrated in a Smart City environment: The gateway should have provision to integrate seamlessly in a Smart City wireless meshed network (a dedicated city-wide network to manage urban connected devices such as meters, waste bins, parking sensors, traffic lights, pollution sensors).
14. Remote management: The gateway must be controlled and managed remotely
15. Seamless installation and commissioning: The gateway must be integrated seamlessly and automatically to an existing network. The gateway must communicate seamlessly and automatically with an existing gateway
16. The gateway should support the controllers/nodes roaming feature for redundancy and seamless installation purposes.
17. Maximum number of nodes supported by the gateway
18. The gateway should be able to at least manage 200 nodes/controllers
19. Communication specifications:
    - 256bit AES encryption for the broadband communication
    - 128bit AES encryption for the narrowband communication
    - Radio modulation: BPSK, DBPSK, QPSK, DQPSK, 16QAM, 64-QAM, GFSK, FHSS Full duplex communication
20. Fully meshed wireless, self-configuration and self-healing features on the narrowband and the broadband networks
21. Depending the number of LCUs ensure good network performance care should be taken that the adjacent mesh network use a different radio channel
22. On the stack side Low Power Wireless Personal Area Network like 6LoWPAN can be used to make a mesh network among multiple LCUs
23. Data should be stored temporarily of connection is not established with CMS Server and resend the data when the connectivity is available
24. The communication channel should be able to handle other data communications as required by other components of the pole

C. Light Control Unit (LCU)

1. The LCU can be retrofitted into an existing street light or added as part of a new street light, providing the ability to control, configure and monitor the street light
2. The various control features provided by the LCU are ability to Turn ON/OFF and Dim the intensity of the street light.

3. The LCU also measures the Voltage and Current at the street light and transmits this information to the CMS periodically.
4. The LCU can continue to switch on-off the individual street light using the last received scheduling information to keep the system working even if the network breaks down.
5. Optional metering IC to measure power consumption
6. Remote management: The Luminaire Controllers must be controlled and managed remotely.
7. "Seamless installation and commissioning: The Luminaire Controllers must integrated seamlessly and automatically to an existing Luminaire Controllers network.
8. The Luminaire Controllers must communicate seamlessly and automatically with an existing gateway. The Luminaire Controllers must be able to roam between gateways for redundancy and seamless installation purposes

D. Central Management Software:

1. **Intellectual Property:** The technology needs to be owned completely (100%) by a single vendor
2. Multi-User Web Application Server the CMS shall be based on an open Web Application Server. Its user interface shall be 100% Web-based and accessible from any computer on the network through a Microsoft Internet Explorer, SAFARI or Chrome web browser
3. Enterprise server The CMS shall be installed on a server that belongs to the organization/customer or to one of our local service or IT sub-contractor. Cloud-based, SaaS model or any server that is web-hosted by a Bidder of a part of the solution is not accepted. It should support any one in its whole
4. 100% Web Interface Web user interfaces shall run and be supported on Microsoft Internet Explorer, SAFARI and Chrome on WINDOWS-based PC and MAC OS and also on Mobile devices.
5. Mobile devices that can access the interface should be pre-configured
6. Based on open technologies The CMS must be developed with open and standardized languages including Java, XML configuration files and SQL database. It shall enable the development of additional features without the need to acquire any development software license.
7. Open database engine The CMS shall record all the data in a centralized SQL database and shall be compatible with MYSQL to avoid being obliged to purchase additional software license for database engine
8. User authentication system The CMS shall enable administrator to create, modify and delete users, passwords, groups and access controls.
9. The CMS shall automatically close connections after X mns (configurable) of inactivity.
10. Tiered level access and management

11. Integrated CMS: The CMS shall be an integrated and ready-to-use application that does not require any specific development before being deployed.
12. The CMS should be a flexible and modular application, supporting the management of any type of Smart City services: a dedicated city-wide central management system to manage all types of urban connected devices such as meters, waste bins, parking sensors, traffic lights, pollution sensors.
13. Support multiple types of Control Systems, i.e. Gateways The CMS shall manage and communicate with different types of network devices as listed in the previous sections (gateways, nodes)
14. It should also support different heterogeneous Control Systems, including power line systems and wireless systems
15. Network management The CMS should support and enable:
    - The management of the narrowband networks
    - The management of the broadband networks
    - The management of the applications
    - The management of the networks configurations
    - The management of the data generated by the nodes and gateways (network data and user data)
    - The Monitoring and configuration of network objects
    - The management of the network links and provide link status, link quality and link reporting
    - Detailed broadband network reporting: wireless transmission power, TCP/IP usage, link utilization
    - The management of the network as a whole, with network status and network quality
16. The CMS should provide automatically or on request, the status and the related critical events of each managed objects. Those critical events could be: wireless link quality, usage of the objects, outages, battery life-time
17. CMS shall provide a user and object management system The CMS shall provide ways to create user profiles, users and access rights to web applications as well as to groups of objects.
18. The CMS shall manage the objects individually or by groups of objects"
19. CMS shall log all actions The CMS shall log all the actions from all the users.
20. Recording Node and device history (linking network Nodes, lamps/meters, customer accounts) and keeping track of adds, moves or changes
21. CMS shall provide map-based inventory features The CMS shall enable users to group objects per geographical zone, to move objects, to delete objects and to duplicate objects on the maps.
22. The CMS should display the network topology (objects, links, status) on a map, in a tree format, and other graphical views to ease the management of the network

23. CMS shall support multiple types of objects, enable new attributes to be created and provide inventory import/export features. The CMS shall support Light Points, Segment Controllers, Sensors, Electrical Vehicle Charging Stations, Weather Stations, Energy Meters and other types of objects.
24. It shall enable the import/export of the inventory in the following formats:
    - Standardized CSV formatted file
    - ODBC and text export
    - Via the XML server
    - Via SQL queries into the database.
25. Configuration of all the parameters of the Gateway and the nodes The CMS shall enable end-users to configure all the parameters of the Gateway and the nodes, including the IP communication parameters, astronomical clock, real time clock, schedulers, Gateway's inputs/outputs and associated scenario, etc.
26. Auto-discovery of the networks' objects.
27. Management and configuration of the services The CMS shall enable the management and configuration of the Smart City services, such as the street lighting, parking spaces, meters
28. Automatic installation process: The CMS shall provide end-users with processes and tools to automatically process the installation and configuration of the Nodes
29. Gateways shall "PUSH" data to CMS. The data logs (all data read by the Gateway on the Nodes) generated on the Gateway shall be pushed by Gateways to the CMS rather than pulled by the CMS to provide a higher scalability. The data collection process shall not require any manual operation. The data presented by the CMS (related to the network or the services) should be updated dynamically
30. Ready-to-use Web Reports: The CMS shall provide ready-to-use web reports to analyze failures, energy consumption and lamp age. It shall provide a way to display historical values for any measured attribute of any device in the database.
31. Customized desktop of Web Reports and Applications: The CMS shall manage access control depending on the user profile and provide the according list of web reports and applications on a web desktop. Each application shall display only the geographical zone, devices and data that the user is authorized to access
32. "Alarm management The CMS shall enable the administrator to create complex alarm scenario based on the data collected from the Nodes through the Gateways. Such alarms aim at sending only effective alarms to the right end user.
33. The CMS shall perform and support the following alarm features:
    - Receiving/capturing successful/unsuccessful readings from any node-connected devices, at scheduled timings/intervals or on demand;

- Reporting about alarms and status indicators, tamper/thefts, consumption / usage trends from node-connected devices
- Identifying and reporting critical events from Nodes and devices (failures, memory capacity issues, communication link or network failures, power failures,)
- Notify of events via
  - Email and distribution lists
  - SMS
  - The execution of a process by an alarm warning on the CMS

34. Real-time control on maps The CMS shall enable authorized users to control, command and monitor each objects in real-time. It shall provide instantaneous (less than 20 seconds in average) communication (sending commands and/or receiving data) between the nodes/controllers, the gateways and the CMS.
35. Multi-level network topology hierarchy and map visualization to ease the management of the network and the services.
36. Provide web service interface for 3rd party software to leverage the CMS features The CMS shall provide with XML, API and SQL access as well as a set of web service interface to enable third party authorized software to use the CMS features.
37. Maximum number of managed objects The CMS should be able to support and manage an unlimited number of objects
38. Backup server and server farms: The CMS should have a backup function with a live standby server and automated failover
39. The CMS application and the SQL database should be able to run on different servers, if needed, to manage growth.
40. The CMS application and the SQL database should be able to run on their respective server farms, if needed, to manage growth.
41. Any update to CMS should not tamper the application in production
42. ITIL based Service Level Management application and Integration with MSI

E. Pole

New poles are not required to install. If existing pole does not support to add the Smart elements, then prior permission to be taken from VSCL to procure new poles

4.8 GIS Maps for real time integration with all Smart City Elements

MSI would analyze the integration of all mentioned Smart elements in the RFP with Varanasi GIS maps and provide operations that help achieve KPI's mentioned in the RFP for each of the Smart elements. MSI should conduct analysis of integration points and provide a detailed report and get approval from VSCL before integration. It should also include elements mentioned in functional and technical requirement of e-governance & utilities. MSI is responsible to work with the vendor to get the GIS Maps and integrate (Geo tagging, Geo fencing etc) with Smart elements. VSCL will help MSI get the details from each line department and facilitate to get the required information on time. MSI shall develop operational procedures using GIS Map Interface.

GIS Map will be provided by VSCL on ArcGIS for integration. All the smart elements should be integrated with the GIS Map

1. GIS Map should be used as a common platform across all the solutions including Smart parking, Environmental Sensors Monitoring, Intelligent Traffic Management, Smart Street Lights, E-Governance, Utility Management system etc.
2. Appropriate geo referencing & geo tagging on the map should be done covering all relevant Smart elements in the RFP and various POI's such as public amenities, bus stops, bus routes, bin locations, transfer stations, street poles etc.
3. The component mapping should be multi layered keeping in vision the requirements for next 20 years.
4. GIS data modal need to be designed in accordance with Smart City solutions and need to be scalable and robust in nature so that it can meet any future need of smart solution and integration with future smart solutions and modules of city
5. Alert, Events, Statuses for each smart element including hardware and software should be displayed on GIS Map
6. The related Smart elements like Variable messaging system should also be displayed in the same layer for the application. Ex: Smart Parking, Traffic Management, Environmental monitoring, All the details should be real time by integration with Variable Messaging System
7. All government buildings and spaces should be geo tagged for the City of Varanasi
8. GIS data modal integrated should support domains, subtype, spatial rules and relationship, joins and spatial references etc.
9. GIS catalog should be used to manage and maintain the GIS data modal. It must support database administration for user creation and management for GIS database

10. City Level GIS Portal: GIS Web will include city portal for as a single window for accessing all the location based information. For more details, please refer to KASHI SMART CITY MOBILE APPLICATION
11. There must be grievance reporting functionality that is associated with ward. This interface must allow citizens to enter the description and detail about the grievance that can be submit to respective city authority.
12. GIS Maps should also display grievances status for all the Smart elements geo tagged on the Map
13. There must be proper workflows for authority /administrators to manage, approve and reject the request from public crowd sourcing.
14. GIS system must allow administrator to manage the citizens submitted grievance reporting and request from public crowd sourcing interface.
15. Department specific search & query module should produce relevant output
16. SWM Assets mapping on GIS such as bins, transfer stations, landfill, garbage collection sites etc. Authority will provide SWM department related data.
17. GIS maps must be integrated with GPS devices to locate real time position on GIS map & provide optimal route mapping
18. There must be various analysis and work operations for Solid waste management from GIS application such as Geo fencing of waste bins, Geo fencing of vehicles, locate bins and bins location, signals, CCTV Surveillance cameras and provide planning & route optimization.

4.9 E-Governance

A. Smart Kashi Portal & Smart Kashi Mobile App

Smart Kashi Mobile App

Varanasi Activity advisor app (Kashi Mobile App) will be one stop solution where the user can opt for multiple activities available in Varanasi. From Eateries to Temple Tours and famous attractions, this app envisages to cover any and every activity offered in Varanasi. This app will also be a location based app. For e.g. a citizen can access the app from any location in Varanasi and know about the nearest available activities that can be availed.

How it will work

Services offered by Private tours and travellers, tourist guides and government services will be registered on the application.

Varanasi Activity Advisor App will act as a medium to register the services and give accessibility to the user to book the service.

The user can avail the services by giving a nominal service fees (15 Rs) which will be helpful for the government for revenue generation.

The MSI will create and host a Web portal & Mobile Application for Department with the following features:

Audio, video, image and text information about the following:

a) "About Varanasi/ Kashi" will provide details about Varanasi city and will have dedicated sections for about the Varanasi city, history of Varanasi, how to reach, climate, local cuisines, festivals of Varanasi, Important Business locations, places of interest, art and craft, facts at a glance, where to stay, where to eat, places of interest, heritage spots, weekend getaways, nature discovery, farm tourism, places to visit, best time to visit, gallery (Photos & videos), etc. few of these points have been elaborated below in detail
b) "Explore District" giving details about the districts, history, how to reach, cuisine, festivals, Important Business locations, places of interest, art and craft (Add to Favorite, Get Directions, About, Get There, nearby and each linked with Google Map and Photos of concerned location).
c) "Facts at a Glance" giving details about area, population, currency, religion, linking roads, postal code, longitude, latitude, area, altitude, population, literacy rate, STD code, average rainfall, villages, language and best season to visit
d) "Tourism destination" giving details on tourism experience (Add to Favorite, Get Directions/Driving Directions, About, Get There, nearby and each linked with Google Map and Photos of concerned location) heritage spots, pilgrim destination, nature discovery, heritage, farms, highway, adventure spots, Nearby places to visit, Places to Stay
e) "Tourism packages" including the details of accommodation, tourism and private hotels, descriptions, facilities, tariff, places to visit nearby.
f) "Tourist Places" giving details of Ramnagar Fort, Sarnath Museum, Ganges river puja, Chandra Prabha Wildlife Sanctuary, Bharat Kala Bhavan, Deer Park, Kashi Vishwanath Temple, Manikarnika Ghat, Dashashwamedh Ghat, Dhamek Stupa, Sarnath Museum, Gyanvapi Mosque, Chaukhandi Stupa, Chandra Prabha Wildlife Sanctuary, Sankat Mochan Hanuman Temple, Prachin Hanuman Ghat, Bharat Kala Bhavan, Durga Mandir, Varanasi, Bars and Clubs etc.

g) "Where to Eat" Section with detailed listings of various eating joints including those in geographical proximity using google map functionality (i.e. Restaurants around Me). Also show Travel Distance (length of time in mins and km or miles) via walking, driving to the listings.

h) "What to Do" listings, including listings in map using Google map API functionality. Also show Travel Distance (length of time in mins and km or miles) via walking, driving to the listings.

i) "Events and Entertainment" with a focus on what is happening and available that evening. May include the ability to add to user's calendar.

NOTE: Content for the application and sections mentioned above will have to be created/updated by the implementing agency in consultation with VSCL or whomsoever that may be decided later by VSCL. The content on the mobile application should be available in Hindi and English language.

- Fare details for taxi, auto and other public transports details.
- List of helpline numbers like police, hospital, women's helpline, transport etc.
- Mobile applications should be developed as native app
- Twitter / Facebook Feed Integration and Sharing
- Navigation path to the destination selected by the user
- Orientation and navigation (using smart phone GPS capability)
- Push notifications to users with ability for the user to Accept / Decline receiving these notifications;
- Turn notifications On / Off
- Integration with payment gateways for payment of cab, hotels etc.
- Ability to add various items to Favourites
- Ability for users to rate the App and to add / surf comments
- Ability for users to share their comments with friends and networks via Facebook, Twitter YouTube channel & Google Plus
- Application should be user-friendly
- Mobile app solution should be scalable to allow for easy upgrades in future
- Offline content is required to offer users a rich experience without worrying about incurring roaming charges
- Emergency contact numbers and SOS feature
- It is envisaged that this application would be downloadable for free from the appropriate Google Store, Apple store, etc.

Modules to be covered

The App will act like a medium to register any activities offered by the registered guides, tours /travel companies or offered by the Government. This app leverage the tourism of Varanasi in a more systematic manner. The broad features too be identified in this app are the following:

Modules	Sub - Modules	Remarks
Shopping / Handicraft Attraction	Brass Ware	This will be static data however will be GIS location based. For e.g. if the user wants to know the area in the surrounding then the list of shops will be displayed with the direction as to how to reach there.
	Copperware	
	Ivory Work	
	Glass Bangle	
	Wood, Stone & Clay Toys	
	Exquisite Gold Jewellery	
	Banarasi Sarees	
	Bhadohi Carpets	
Tours	Day Tour	This will be dynamic data and will be controlled by the Private Tours and Travels or the Government. For e.g. the travel and tour company will have the flexibility to publish different schemes on the portal.
	Ganga Aarti tour	
	Temple Tours	
	Ghats	
Performances	Music & Dance	This will be dynamic data as well. Like Book My Show application.
	Art Galleries	
Places to Eat	Restaurants	An initial survey of each ward will be done to map the longitude and latitude of the famous eateries in the city.
	Banarasi Pan	
	Cafes	
Yoga & Meditation, Spa & Rejuvenation	Yoga Houses	This is one of the most upcoming activities in the country. Kashi being hub of Yoga attracts lot of international tourism. All Yoga Houses, Centres will be

		publically mentioned in this app which will facilitate quick knowledge and access to the service centres.
Places to stay	Bed & Breakfast	A list of Bed and Breakfast, Ashrams and Star Hotels will be shown in the application.
	Star Hotels	
	Aashrams & Guest House	

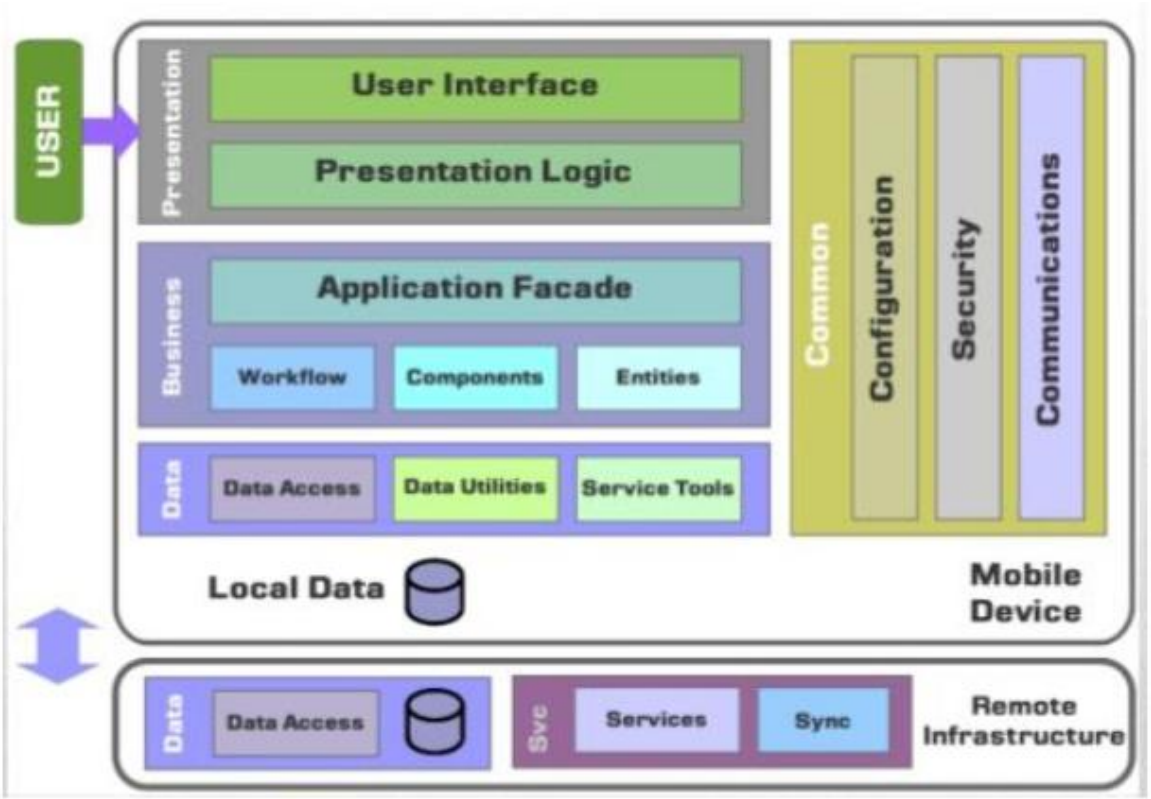
Pilgrim centric services:

The Mobile/Web App which works on LAN/WAN in online/offline mode in integrated manner and must have features like:

- Push Notification on SMS / Mobile App to devotees/pilgrims when they visits city or enter city, Notification should be sent only to those visitors who opt to subscribe the notification.
- Web / Mobile Application should be capable of streaming E-Darshan/ Live Darshan.
- Centralized, Integrated database with Smart City App
- Adhaar Integration with Kashi Vishwanath Temple Smart App
- Time slot wise number of registrations,
- System must exclude the times of Aarties,
- there must be proper checking system,
- System must be able to stop fraudulent practices,
- System must meet the peak hours and ideal hours' requirements, (Bidder to propose the hardware requirement to meet the concurrency of 30,000 User.)
- System must ensure to complete the Darshana within stipulated time printed on the tickets,
- easy record keeping and retrieval system,
- The access card be printed with reporting time/date/and gate no. for darshana, and card should not print without capturing photograph of devotees/pilgrims
- easy access and quick disposal mechanism on queue verification counter,
- System must be capable to capture devotees/pilgrims data finger/photo and allocate the slot for Darshana,
- System must be capable of track record of the missing person in real time and report should be generate within a minute and just the touch of the finger his name should remove from missing person list,
- System must be capable to centralized registration of devotees/pilgrims,

- System should be capable of sending timely notifications to the pilgrimages in regards to their Darshan time schedule
- System must be capable with 20 barcode/QR code technology,
- System must be capable to prepare emergency response plan,
- must me capable to search pilgrim name wise and token number-wise,
- must be capable to manage any delay happens due to unforeseen situation,
- must be capable to manage let coming devotees/pilgrims
- must maintain the DR system and any failure shall be managed within a minute time.
- Must be capable of printing priority access cards
- works on LAN and VPN,
- the Application must be capable to show real time data that how many devotees/pilgrims are inside of the temple exist based on a particular time how many access cards issue minus how many devotees/pilgrims exit from the exit gates, and this data should be available on the display boards as well as in the control room and hourly report send to temple administrator as well as police choki.
- The Application must be capable to keep record of different hall as well as its capacity, as soon as the devotees/pilgrims capacity increases to hall the capacity he has to inform to the devotees/pilgrims through SMS or announcement about the place where he has to wait and how much time they have to wait.
- The Application must compatible to capture the biometric records of devotees/pilgrims and it should also get the pilgrims data from his/her adhaar id.
- All the reports and access cards shall be print in local languages as well as in English

Reference Architecture for Mobile App



Points of Interest:

The portal shall provide information about key point of interests in and around every destination of the city. The point of interests shall include local attractions, shopping places, cafes, restaurants, currency exchange centers, souvenir shops and emergency services like dial 100, tourism police and hospitals. The user shall filter these POIs based on the categories and distance. By default all the point of interests related to a destination shall be listed.

GUI (Graphical User Interface) based Integration:

The application should have an integration with the GIS maps for the city/ Maps of India/ Google Maps which allows the end user to locate the point of interest on the map and show the direction to reach the destinations accordingly. The application should have provision of location based services. For e.g. the application should have the feature to filter the nearby places/ activities as per the current location of the user.

User interface requirements

- All icons must be crisp, clean, and distinguishable and should be as per guidelines of Mobile Application Platform.
- All buttons and objects must be reactive to touch and work as intended.
- All functions must stay within the mobile platform boundaries.

Integration ad Aggregation of services:

Integration and aggregation of innovative 3rd Party citizen centric services provided by private companies that are relevant for citizens shall be facilitated. The 3rd Party services will be identified and evaluated by either Smart City PMU team and shall be integrated by the Partner Agency after consultation with VSCL. These services will need to be incorporated with the envisaged system architecture through Service Oriented Approach available for application servers deployed at Data Center. As per the guidelines to be published, these can be integrated into the mobile app or other mobile channels based on the technical feasibility.

Integration with other Mobile Applications:

Kashi Smart City Mobile Application (KSCMA) platform and mobile app, in addition to the services on-boarded through the platform, shall have functionalities to integrate with mobile applications separately developed by various government departments. The KSCMA mobile/web application should, provide a directory listing all such mobile apps through KSCMA platform with a link to:

- Invoke the app if the app is installed in the user mobile or
- Trigger download of the app from the app store where it is hosted.

In case of the module to check for hotel prices, reservations – the app should be compatible to fetch data from various available Portals / Mobile Apps from private players like Make My Trip, Booking.com, trivago, etc. for Hotel boarding and accommodation facilitation for pilgrims, visitors to the city.

Survey of the Area:

The application is envisaged to be a medium where the tour operators, points of interest and hotels will be self-registered. However, the survey of the place is required by the bidder to be done to map at least 50 points of interest from each category listed above before the launch of the application.

Booking System through Application:

Booking system shall help travelers planning to visit Varanasi to book flights, hotels, holiday packages and other services online. The Booking system shall be provided on the home page of portal for easy access to bookings.

It shall also be integrating with payment gateways for reliable and secure payments.

The booking system shall fetch Real Time inventory of flights, hotels, cars and buses. The system shall have provision to build special offers, top destinations and featured holiday packages to display on homepage. Registration and membership option for users shall also be available. Secure authentication via HTTPS shall be ensured for all booking modules.

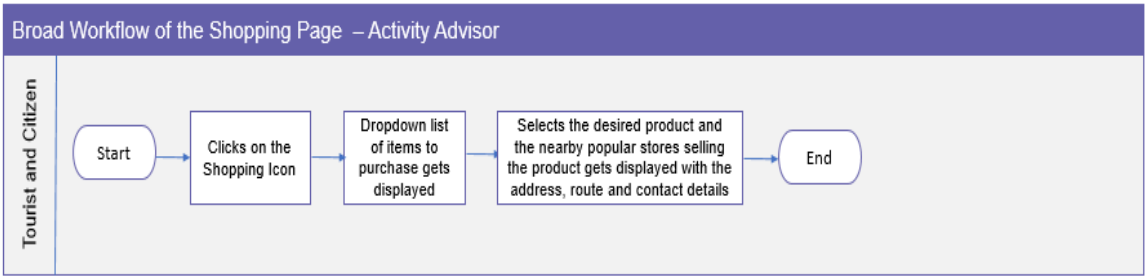
Rewards/Loyalty Program Integration:

To encourage travelers to continue planning and booking their travel with this portal a customer reward/loyalty program shall be integrated with the solution. This program shall incentivize travelers with some benefits e.g. discount coupon, additional services etc. on the basis of spends and other parameters.

Workflows for the identified Modules:

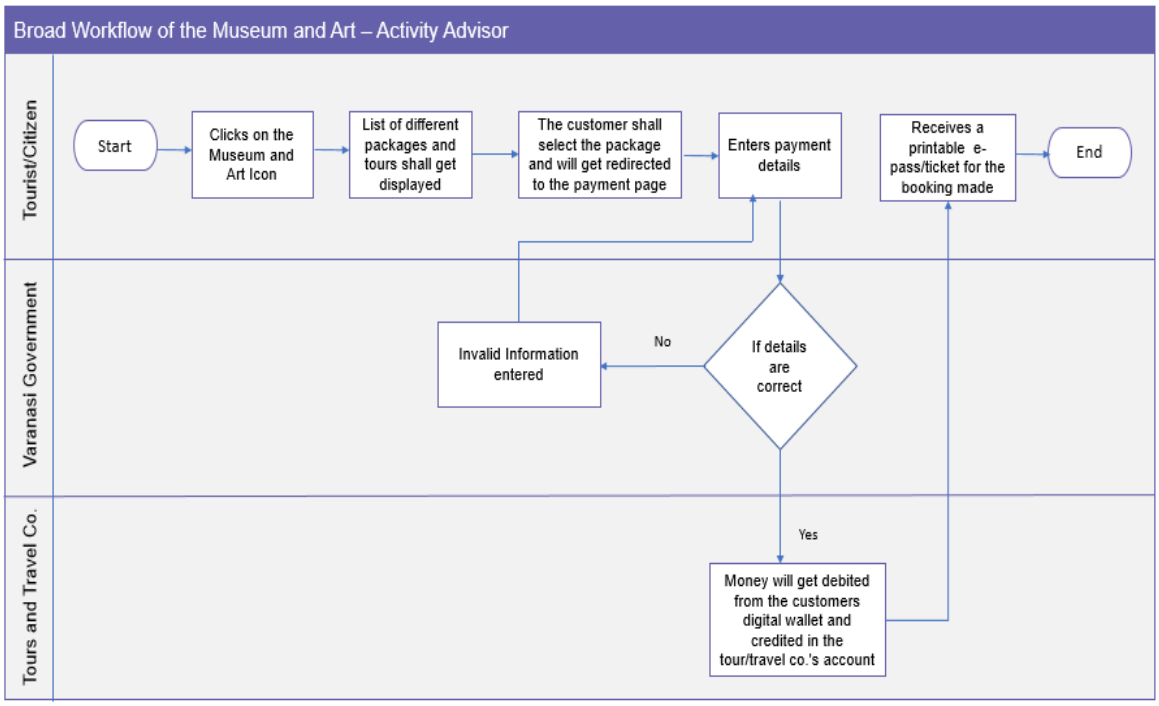
Shopping Module

- A dropdown list of the different products available in Varanasi will get displayed on the user's screen to choose from.
- After the citizen/tourist chooses the product, information about the product shall be visible to the user and a page of the nearby stores selling the product with the address, contact information, route via google maps etc. will get displayed on the screen.



Museum and Art Module

- The list of the different packages offered by different tours and travels/ department with a guide option will be available to the user.
- After the user opts for any of the packages, he/she will get redirected to the payment page.
- The user shall enter the details and make the payment via the digital wallet account.
- The Payment will reflect at the Govt Server for authenticity.
- After the Payment gets approved the same gets received by the Tours and Travels company.
- The e-ticket of the package booked will get mailed to the end – user.

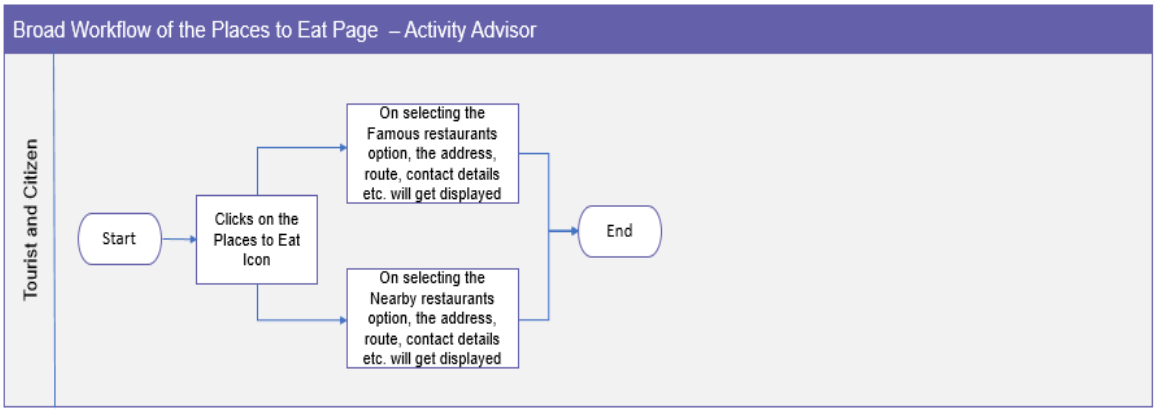


Events and Performances Module

- The list of the different events being held with the schedule will be available to the user.
- After the user opts for any of the programs, he/she will get redirected to the payment page for booking.
- The user shall enter the details and make the payment via the digital wallet account.
- The Payment will reflect at the Govt Server for authenticity.
- After the Payment gets approved the same gets received by the Varanasi Govt.
- The e-ticket of the package booked will get mailed to the end – user.

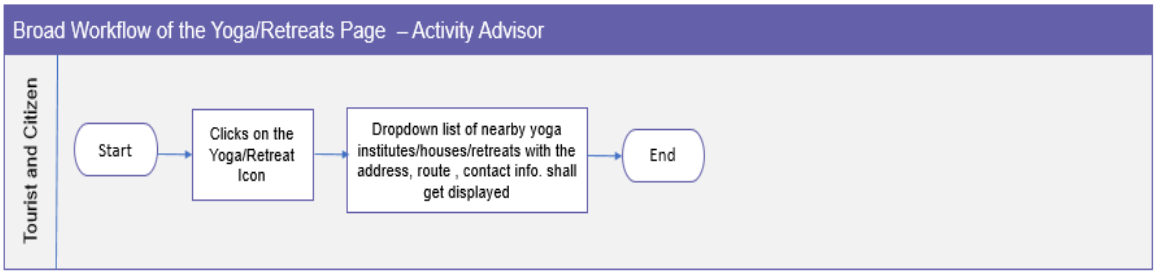
Places to Eat Module

- After the tourist clicks on the Places to Eat icon, 2 options get displayed on the end user's screen.
- Option 1: The list of the Famous Restaurants in Varanasi shall get displayed with all the information like how to reach, address, contact info etc.
- Option 2: The list of the Nearby Restaurants in Varanasi shall get displayed with all the information like how to reach, address, contact info etc.



Yoga/ Retreats Module

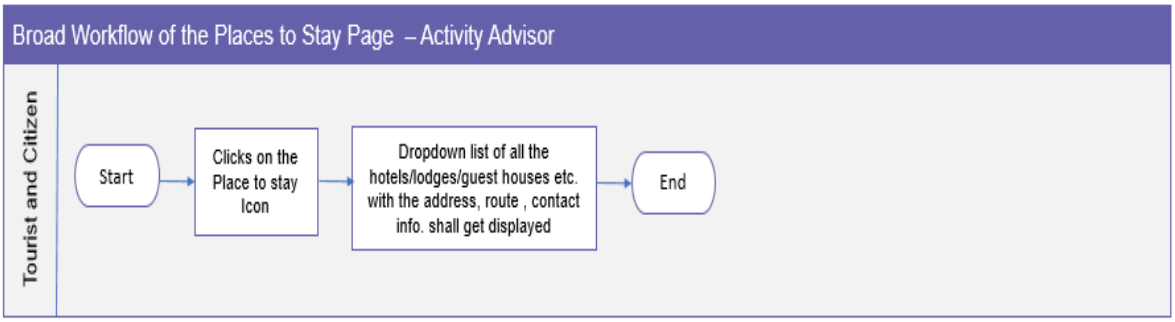
- After the tourist clicks on the Yoga/Retreats icon, the information on All about yoga in Varanasi gets displayed along with dropdown list of the famous yoga houses on the end user's screen.
- The user will also get an option on how to reach the yoga houses and Spa centers.



Place to Stay Module

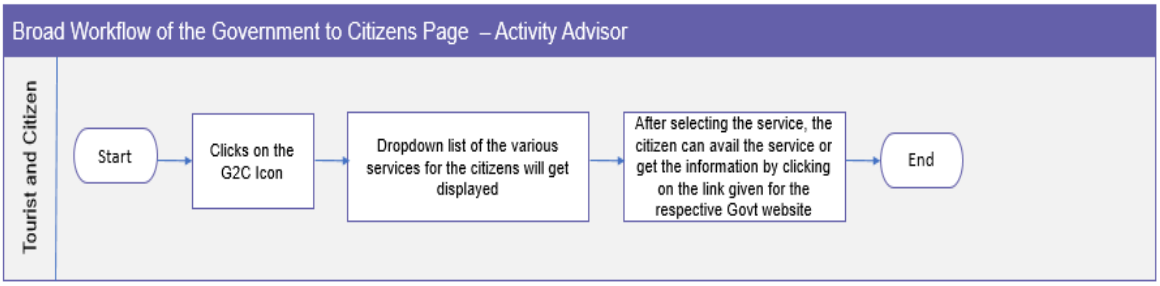
After the tourist clicks on the Places to Stay icon, the information on all the hotels/lodges/guest houses etc. gets displayed along with the rating, address, contact info, route etc.

Note: This module will have an integration with the available API for the private third party application, where the user will have the option to be routed to the specific private player mobile application, wherever the listing of the hotel is specified. This module should search at least three major private players available in this sector.



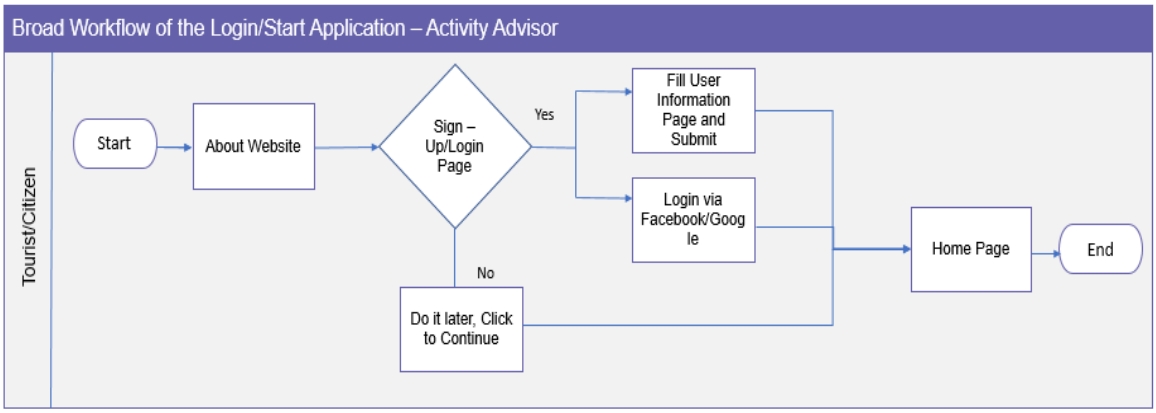
Government to Citizen Module

- This Page shall reflect the different options available for the citizens.
- The Citizen can choose the service he wants to avail for e.g.: check aadhaar status.
- The User can click on the link for the aadhaar status will be available on the Portal / Mobile App and will redirected to the desired page.



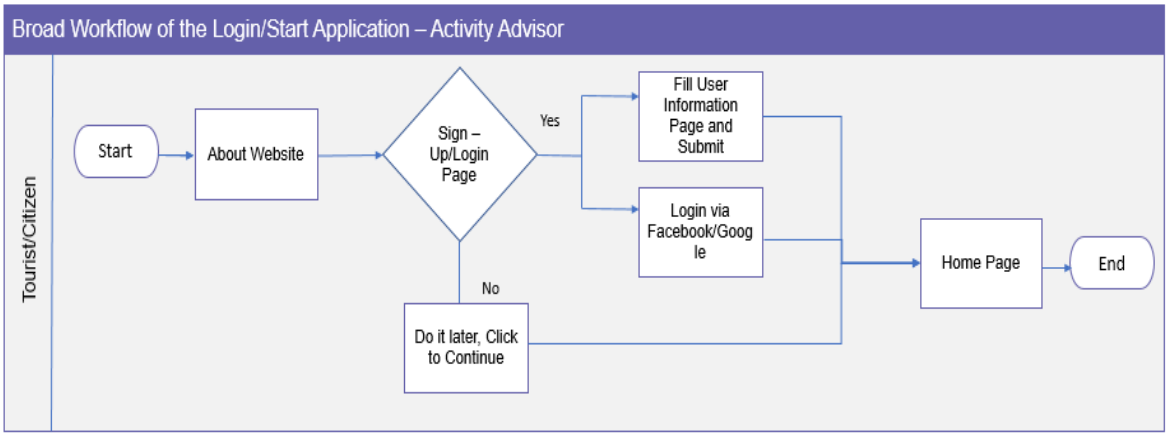
Application for the end user:

The Tourists/Citizens will have an option to register or link the account information through face book or Google to access the various facilities through the Portal / Mobile App. The tourist/citizen shall have the option to choose or view the information in an interactive audio, video and images format.

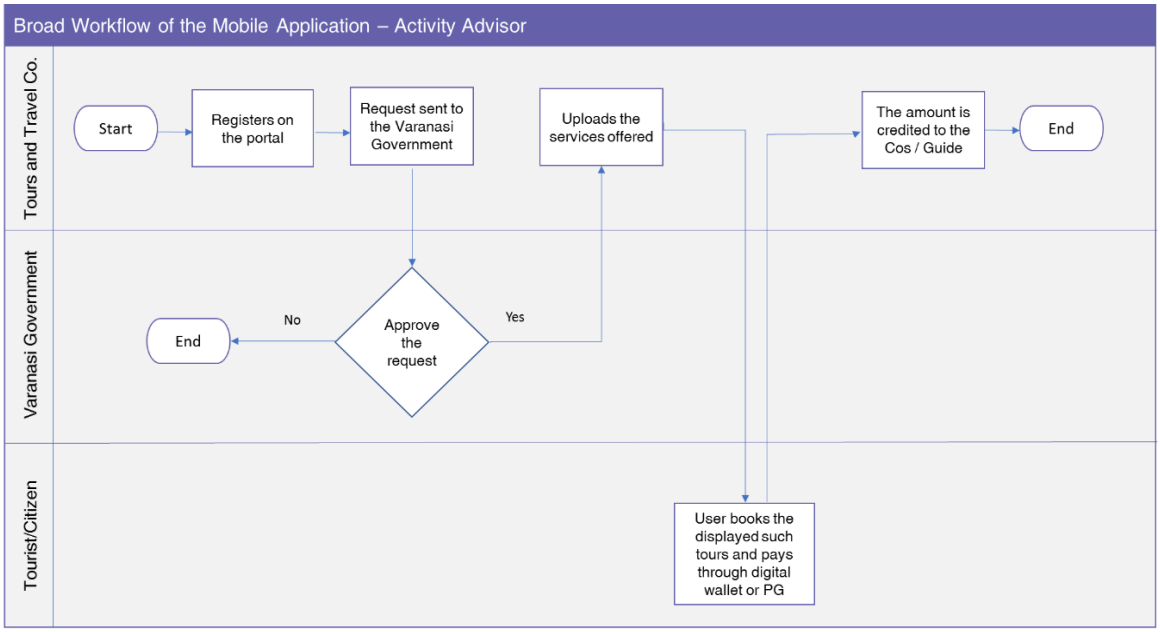


Application for the registered vendors

An application to register the government services and to register the vendors will also be developed. Through the application the registered vendor can add/modify/delete any of the activities. Whenever there will be a booking generated by the citizen or the tourist, the request will be generated at the respective vendor. However the registration of the vendor will only be approved by the Government.



Workflow of the overall application



E-Governance for integrated system at KICCC:

Admin User- Content Management Functional Requirement Specification

This section lists the specific end functionality as well as the requirements for all aspects of the admin user-Content management tool. To manage all mobile application contents, separate user friendly content management system (CMS) tool needs to be developed.

General Design Guidelines for CMS Application

Following list will provide the general guidelines followed for CMS application design.

1. User should be able to create, update, publish/unpublished and delete the data.
2. User should be able to search the data.
3. User should be able to sort the data.
4. CMS should support two levels of user.
    a) Admin User - Can perform all the CMS functions.
    b) Normal User - Can perform all the CMS features except Publish, Delete and editing any record in the system. Normal user cannot create any new user.

5. CMS should be protected using HTTPS for secure access of information and access for CMS users

Reporting Requirements

As per the requirement of VSCL, following reports will be needed for the Admin:

1. Audit Log Screen will be provided to admin user to check the activities performed by all users. The data will be available only in read-only mode.
2. Admin User will be able to see the list of login/logout information for the user through Authentication report screen.
3. Admin User will be able to see the list of notifications sent to the devices through notification screens. Data will be only in read only mode.

   Google store, Apple store, etc. dashboard details regarding total downloads, crashes, uninstalls, etc.

Traffic Monitoring

Citizen can access the GIS Maps/ Maps of India/ Google maps or any third party maps to track the traffic of the desired route. The user should have the feature to set indicators on this map. For e.g. User should be able to receive push SMS whenever there is less traffic on the selected route as per the requirement.

Smart Parking

The user should be able to launch the smart parking module through this application. The application should show the available and filled spaces at a particular vehicle parking area on real time basis. The application should have the availability to book a slot through this application from his location. Feature of Advance booking shall also be made available. However, the user should be allowed to book the parking 2 hours prior.

The data of the smart parking will be received through the application/ SMS services through KICCC feeding inputs (via sensors placed in the designated parking lots in Varanasi).

Emergency Services

The Scheme of Women/Senior Citizen/Citizen/Tourist Helpline is intended to provide 24 hours immediate and emergency response to the citizen affected by violence through referral (linking with

appropriate authority such as police, One Stop Centre, hospital) and information about women/senior citizen related government schemes programs across the country through a single uniform number.

This helpline is exclusively designed to support citizen in distress facing violence or threat of violence, both in private and public places, including in the family, community, workplace, etc. The Helpline will provide a 24-hour emergency response.

All existing emergency services and those that provide support to citizen would be integrated with this helpline. All the city level helplines whether private or public would be integrated with this helpline.

General Instructions

- The helpline staff shall at all times be extremely polite and give a patient hearing to the caller.
- The helpline staff should reassure the caller that help is on its way.
- The helpline staff shall not insist on the caller disclosing his/her identity, unless the caller so agrees and should assure the caller that the confidentiality of his/her identity and contact information shall be maintained.
- A confidential record including identity and contact details of the caller (if provided), along with aggrieved woman's personal and case details and name of the officer to whom information was passed on with date and time will be fed in to a system as per the prescribed format and a Unique ID Number would be generated.
- As soon as the complaint is registered a call/text message (SMS) would be sent to the SHO/ DM/ SP/ DYSP/CMO/PO/DO of the district/area as required.

This command and control center should offer services in the following four categories to any woman or girl facing violence within public or private sphere of life or to any citizen seeking information about any government or general programmes or schemes:

- Information services
- Enquiry Services
- Request Services
- Grievances & Resolution

General Requirements for Emergency Services to cater immediate requirements:

- To create a fully equipped & integrated Helpline for Varanasi
- Help in preventing, detecting and dealing with criminal activities with minimum turnaround time
- Provide alerts to the concerned department after the ticket is locked for emergency services. .
- Monitoring of suspicious people, vehicles, objects etc. with respect to protecting life - and timely informing the citizen, local authority
- To setup multiple seated command control center which can be scalable in future.
- The MSI shall provide a web enabled helpdesk management system with SMS and email based alert system for the Helpdesk Call management and SLA reporting.
- Availability of multiple channels to log a complaint such as Toll-free lines, landlines, helpdesk tool, E-mail, direct walk-in etc. Outage of any component shall be calculated as a time between logging the call and closing the call.
- To acquire toll free number and provide **toll-free 24-hours telecom service** to women/senior citizens affected by violence seeking support and information in Varanasi.
- **To facilitate crisis and non-crisis intervention** through referral to the appropriate agencies such as Police/ Hospitals/ Ambulance services/Protection Officer (PO)/OSC.
- To provide **information** about the appropriate support services, Government schemes and programmes available to the woman/senior citizens affected by violence, in his/her particular situation within the local area in which the citizen resides or is employed.
- Important features include:

1. **Command and Control Centre EPABX solution features:**

   The Gateway should have the facility of accepting PRI connection, more than 5 extensions as per the below mentioned features.

2. **ACD (Auto call Distribution)**

   The ACD Key Features includes ANI/ DNIS based routing, managing multiple Queues, Welcome greeting message, Office hours configuration, Compliant with standard PBX, Media Gateways & Phones, Different user defined reports, Web access facilitating remote agent login, Skill-based Call Routing, Wait time notification and integration with calendar & Voice logger. Also have the ACD Queues facilities.

3. **IVR (Level-3 Voice Messaging)**

   Level-3 IVR should have Self-help service with Text to Speech and Automatic Speech Recognition, IVR Node Flow Designer with Scripting Capabilities, Multi-language Support, Email/SMS/Fax Integration, Customizable IVR prompts and Agent Greetings facility.

4. **Call Centre Communicator**

   The CCC should be GUI based. It includes VoIP Soft Phone, Instant Messaging Client, Operator Panel, Conference Administration, pop-up agent workbench screen, Unified Customer Interface for call handling, Call disposition, Conferencing, N-way Call Transfer and Missed Call Alerts

5. **Real Time Agent Monitoring**

   The Solution should be provided with facility of Barging, Listening and monitoring the calls.

6. **Voice Logger**

   There should be provision of Pre-Integrated Active Voice Logging, 100% Blind Recording, Multi-format Voice Recording, Automatic Compression and Archiving and Web-based Remote Access to Voice Logs. Facility for quick and easy retrieval of Voice file according to the calls made.

7. **Gateways**

   Centralized Gateways at Varanasi shall route all the calls received from any service provider to the Command & Control Centre through 2 PRI lines provisioned for Inbound. Another 2 PRI lines need to be provisioned for Outbound Calls.

8. **Supervisor Application**

   There must be the facility of Supervision architecture on telephony, agent, dialer and lead performance, Independent supervisor interfaces for Inbound & Outbound campaigns and Complete MIS management for device, voice log, services and systems.

9. **Voice Recording & Storage**

   There should be the facility of taking backup of System, Agent, Queue, and Instant automatically with time interval. Graphical interface to maintain the storage location. The implementing agency will maintain the voice recording library. Incoming call recording facility to be implemented for further evaluation of complaints.

10. **CRM Module**

    CRM integration with IVR & ACD should be facilitated to enable customer profiling, Integration with any third-party database, CRM or tool for smooth and seamless functioning and having Web-Agent facility

11. **CTI (Computer Telephony Integration) PoP Up**

    CTI Pop up shall appear on Call taker's desktop along with information of the caller (mobile/landline number and address), which will help the call taker to call back the caller in case of disconnection. This application should be capable of integrating with other applications of the Police dept and scalable to meet the higher performance needs. Application should have the capacity to integrate the tools/application to auto populate the location of the caller once the supporting technology is ready.

12. **Phones**

    Bidder shall provide standard Digital phones for handling the calls. It is advised to have an option to login to ACD through Phone in case of CTI issues & this will be considered as one of the redundancy feature in the telephony. These phones should also have at least 6 party conference facilities.

13. **Head Phones for Call Responders**

    The solution provider needs to facilitate the Head Phones with advance features for the call responders. It should have the facility of Own Dial Pad, Volume Control, Flash Button, Tone/pulse dialing switch, Last Number Redial Button, Mute Button, Over-The-Head Noise-Canceling Headset, Clear Sound quality, Extension Jack

14. **Call Center Statistics**

    The Proposed Solution can able to give Queues/Agents statistics and real time status, Inbound/Outbound Graphs, CSV and PDF Data Export and Windows, Mac, and Linux Desktop Applications support.

Kashi Smart City Mobile Application (KSCMA) Architecture:

Given the differences in the technology with their related advantages and disadvantages and interoperability issues, it is very important to have credible architectural principles to form the basis for choice of a particular technology and architecture to deliver mobile services. Design principles for the KSCMA Platform are given below:

Design Principles for KSCMA

User Centric

End users availing the service must be centric to the design of KSCMA platform. Their ease of interaction with mobile devices, the kind of devices commonly used by targeted segments, network availability and demand for service should guide the choice of technology for service development and roll out. Support for local language (as mentioned in section 4.8 (i)) is necessary.

Heterogeneous and Interoperable

The KSCMA platform should be designed keeping in mind that information flows across applications owned by different departments. The KSCMA platform should be able to integrate

and interoperate with various other external entities. The ability of the solution to easily and in a relatively seamless manner integrate with external entities, interoperate with multitude of technologies is a significant criteria while selecting the technology.

The KSCMA platform should also support features which work seamlessly across various channels providing users a unified experience. Following features should be supported by the KSCMA platform:

- When internet is down or otherwise, the user should be able to make call to the IVR initiated from the App or Mobile Web.
- Call to the customer care support can be invoked from the App or Mobile Web.
- Registration made on Mobile Web will seamlessly reflect in other channels like SMS and IVR based transactions.

Sustainable and Scalable

Architecturally, the KSCMA platform should be sustainable and scalable. Sustainability requires the platform to use softwares, tools, frameworks etc. which has a large usage base and regular long-term support and upgrades. For scalability, it is important for the KSCMA platform to be cloud enabled to take the advantage of next generation cloud implementations and technologies. The following criteria should be kept in mind during selection of the technology

- Every component need to scale to a large volume.
- Every component as well as the whole system needs to provide consistent and acceptable performance even at very large scale.
- Single point of bottle-neck and failure must be avoided. While upgrades and scaling-up, it is necessary that the platform supports earlier versions especially when upgrading the APIs.

Pluggable and Loosely coupled Components

The system should be built with open standards and open APIs with plug-n-play capabilities. The system should be designed to plug-in new technologies and components in a seamless manner, similarly any obsolete technologies or components should be removed without impacting any other component of the system. The components should be loosely coupled to

allow changes in applications that are integrated with it and in any sub-system level without affecting other parts. It should be architected to work in a heterogeneous technical environment.

Easy On-boarding

On-boarding of departments/e-Gov applications should involve minimal changes (ideally to the extent of exposing their existing APIs or developing new APIs if required) in their respective applications. Also, Application enablement should happen seamlessly across all the channels (as opted for by the integrating department) simultaneously.

Address privacy concerns

The KSCMA platform should address the privacy concerns of integrated applications and thus restrict visibility of each department to data/information pertaining only to them. Also, the platform should protect user's information.

Analytics

The KSCMA platform should be able to generate insights for analytics. These includes, but is not restricted to, on-demand reports which can be configured, filtered and customized by Varanasi Government as well as integrating departments. The KSCMA platform should look at the usage at an aggregate as well as at an individual level. Relevant dashboards for admin should be available for decision makers about the platform's performance and usage and insights on user information (demographic, location, behavioural etc. aspects).

The KSCMA platform need to provide extensive parameterized reporting facility for both department users and administrators to run various reports from time to time. It should support MIS reports for all but not limited to the given below items:

- Daily Transactional reports (both for payment and non-payment transactions)
- Consolidated monthly reports for all transactions
- Reports for payment transactions with split of various payment modes like net banking, credit card, debit card, IMPS, Wallet etc.
- Number of hits on various channels (channel wise split) like IVR, Pull SMS, Mobile Web, Smart Client.
- App download report from various app stores
- It should also provide successful and failed transactions

- It should provide service wise reports for Push SMS showing the number of successful and failed SMS from KSCMA
- Any other report as required by Varanasi Government. Analytics functionality should be extended to all the mobile applications, developed separately by a service provider and installed by a user, provided the transactional data of such apps can be pulled by or pushed to the KSCMA platform.

Multi-Language Support

Various mobile channels need to support local Indian languages to be able to reach masses. The Partner Agency shall provide support for English and Hindi , standard local languages across various channels (SMS, IVR, Smart Client, Mobile Web etc) for services across service categories as required by individual integrating departments.

Security and Audit

The KSCMA platform needs to have capability to manage security and privacy at multiple levels. A transactional service may require higher security levels than an ordinary information service such as status check or weather forecast. Non-functional requirements such as data security, user authorization and access control need to be taken into account while designing the components of the platform.

The platform needs to be audited with STQC certification by CERT-IN empanelled agency.

Easy integration with external interfaces

In the current IT environment when several function specific systems are developed, a system comprises of core functional modules talking to several platforms and services through APIs published by such platforms. KSCMA platform needs to have technical capabilities to integrate with external interfaces such as payment gateways, identity providers, location services etc.

There shall be a requirement to integrate the proposed application with other Government department applications or any external application as per the requirement from VSCL. Also, there may be a requirement to integrate the application with other travel applications like www.makemytrip.com, www.tripadvisor.com, www.goibibo.com, etc.

Payment Gateway Integration

To enable hotel booking, air ticket booking, bus booking, package booking and cab booking, multiple payment gateways and popular payment wallets shall be integrated with the solution to give travellers choice of making payments using their preferred medium. The payment gateways/wallets shall have following features: ·

- The payment gateway/wallet and its services shall not be time bound and shall be available to the user 24X7.
- The payment gateway service providers shall provide online payment gateway services with acceptance of credit cards (Visa, Master, Discover, Maestro, and Amex etc.), internet banking and debit cards etc. ·
- The payment gateway shall generate authenticated receipt as a proof of transaction. The system-generated receipt of the payment shall be sent to the payer through e-mail and SMS.

Aadhaar or other identity providers

KSCMA shall integrate with the Aadhaar authentication ecosystem by itself becoming an AUA/KUA or by integrating with an existing AUA/KUA for enabling Aadhaar based authentication on the platform. For non-Aadhaar based authentication, integration with other identity providers such as PAN under Income Tax Department would be required and the KSCMA platform shall integrate with such providers.

Digital Locker

Digital Locker (DigiLocker) is also one of the key initiatives under Digital India program. It aims at eliminating the use of physical documents and enables sharing of verified government issued or self uploaded electronic documents across agencies. Digital Locker provides a dedicated personal storage space in the cloud to citizens, linked to citizen's Aadhaar number or other unique identity. It enables various organizations registered on Digital Locker to push certificates of citizens directly in their Digital Locker in electronic format.

Citizens can also upload and securely store the scanned copies of legacy documents in Digital Locker. A user can share these electronic certificates online with various departments and agencies registered on Digital Locker while applying for the services provided by them. Thus,

Digital Locker brings the citizens, issuers and requestors on one platform. Further, Digital Locker system is based on open APIs which are published on their portal www.digilocker.gov.in . KSCMA shall integrate with DigiLocker and enable

- Submission of documents by a user by fetching URIs from DigiLocker to KSCMA and passing the same to the integrating department service.
- Informing user of any document, related to the service availed on KSCMA, URI of which has been made available on DigiLocker

Private Service Providers:

Bidder shall integrate theee services provided from tour operators, hotel aggregators, food aggregators.

Transaction Management module

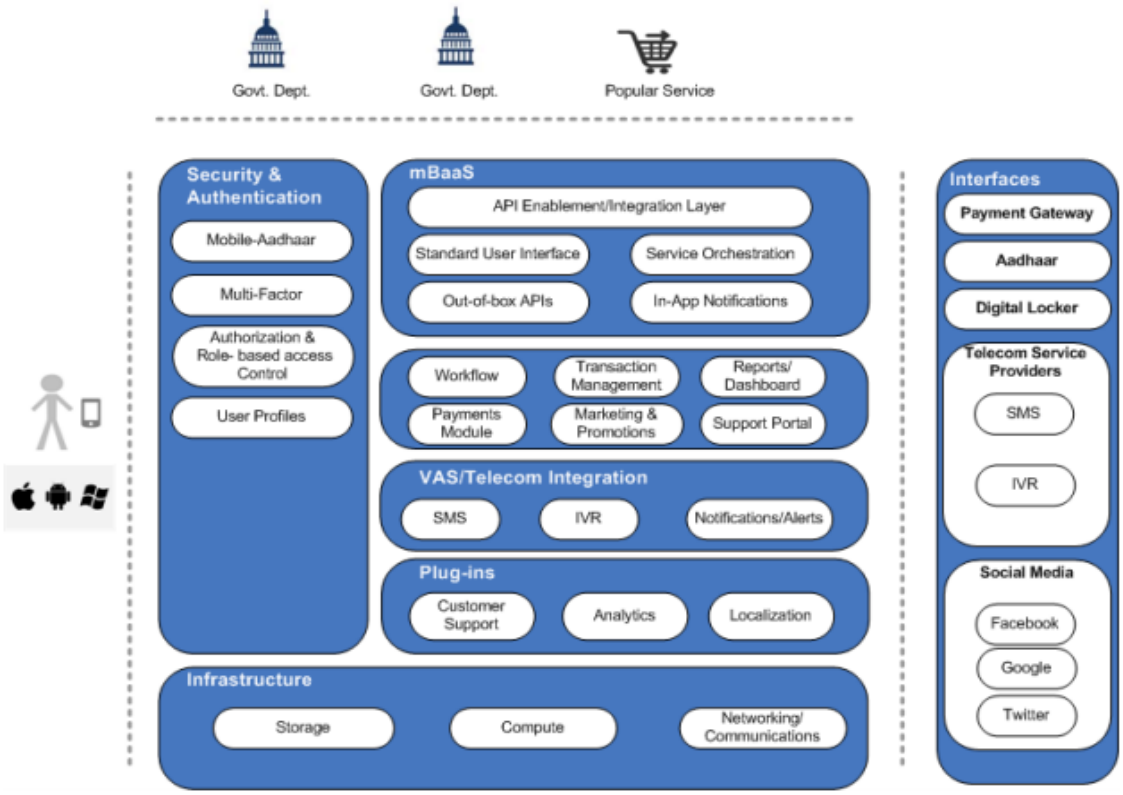
This is the core transaction management module of the KSCMA platform, all the messages will be routed through transaction management module for further processing. Transaction management module will interact with external systems for verification & presentment of the information, will interact with payment module for handing over the information for payment processing, other modules for various types of verifications. Transaction management will also be responsible for calling business rules API for checking various business rules as well as with service charges module for calculation of transaction charges prior to sending the transaction for further processing.

The KSCMA platform should have ability to keep all transaction logs of the users and make it available in a common place as a transaction history. The user should be able to open individual transaction details in a standard format like PDF, html, text or other formats and also can push the details to an email ID/registered email ID to keep an email record and for printout purpose. The transaction history should have all but not limited to the following information:

- Service Name
- Service Department/Company Name
- Transaction ID
- Transaction amount
- Transaction date and time

- Common interface for transaction history should provide transaction trends and graphs for user reference

Components of KSCMA



Integration with Telecom Service Providers (TSPs)

The platform should have network integration modules that support all the protocols used for back-end integration with major Telecom Operators (at least top 5 as per TRAI's subscriber numbers) in and across India for SMS and Voice Channels. Varanasi Govt. will provide support to the Partner Agency in coordination with TSP.

SMS

- SMS Long code/Short code integration and configuration capability with major Telecom Operators as mentioned above.
- SMS Mo(Mobile Originated) Message routing to appropriate service based on the Long Code/Short Code and Keyword.

- Support Delivery Report Tracking and Notification back to the Mobile app.
- Support Multi-modal support for SMS Short Codes.

IVRS

- Long code/Short code integration and configuration capability with major Telecom Operators, as mentioned above, for Inbound Call Services.
- Inbound Call routing to appropriate service based on the user input.
- OBD CLI configuration & integration capability with major Telecom Operators, as mentioned above, for OBD Services.

Mobile Web

Accepting MSISDN forwarding for Mobile Web / Smart Client app for user authentication supported by PIN or alternative methods.

Others

- The platform should have necessary integration to lookup Circle/Operator information by MSISDN.
- Comply with TRAI guidelines.
- Support Configurable retry mechanism based on the error code at Telco Integration Level, Service Level.
- Flexible Traffic Management solution to handle events surge in the usage.
- Support advanced queuing mechanisms to route traffic with different priority as per the business requirement.
- Example: Shall support different queue for incoming/outgoing message forwarding, example: queue 1 is for Service provider 1, 2 and 3, queue 2 for deapartment4, 5 and queue 3 for department6, default queue for others.
- Platform integrations should be configured for High Availability.
- If connection is not available, the KSCMA platform must be able to buffer the messages going to, and handle the additional incoming traffic once SMSCs are up. This buffer must be configurable.
- Changes in the configuration information should not require application restart.

Technology and Server Requirements

- Mobile App development should support Hindi and English language
- Admin CMS application should be developed in PHP/.net and uses MySql/MS SQL open source Database.
- CMS system should be hosted on vendors own data base after completion of project which is handing over to VSCL as per latest technology and Server
- Vendor will setup and deploy Admin CMS application, Web Application on his own server or equivalent cloud based server.
- Vendor has to ensure the development of mobile application as per guidelines issued by Application stores. For ex: Google play, iTunes etc. Vendor has to summit mobile app binary to iTunes app store and Google play store

Customer Support / SLA Monitoring / Application Management

The Partner Agency is required to provide Help Desk module for customer support function, Application Management Module for application management and SLA monitoring. The Help Desk module shall be used by the Partner Agency to manage the customer ticketing and life cycle.

The SLA monitoring tool shall have the ability to track the SLAs which will be described at the RFP stage; the monitoring tool shall have the ability to generate the necessary reports. The SLA monitoring tool shall have the ability to export or import the necessary data.

The application monitoring tool shall help Partner Agency and Varanasi Government manage and monitor KSCMA and related components of KSCMA effectively. The tool shall monitor the services and unified portal.

The Partner Agency should provide an integrated Customer care support interface where the customer care centre can view transactions of the citizen for better coordination and support to the citizen. The customer support should be able to help user in the following ways:

- Inform exact status of the transaction based on his mobile number. The customer care support should be able to recognize the person based on the number he is calling from and get an access to his transaction details.
- UMANG should have a live chat feature for customer support.

Functional Requirements

Portal and App Design and Features

The KSCMA platform should have a robust Configuration and Management system which should allow faster creation and management of desired User Interface and link it to various services and be able to create and make changes to individual pages of the portal and publish these into the production system.

The design of the portal shall be implemented in such a manner that it is easy for the citizen to navigate services as well as to be able to configure favorites services that can be accessed from the home page.

The complexities of interacting with an application on a mobile device, special consideration should be given to the overall user experience. User experience is guided by a number of factors, including: latency, interaction method, and data consistency etc.

Compliance to Guidelines to Indian Government Portal / Mobile Apps

These guidelines have been developed by National Informatics Centre (NIC) and adopted by Department of Administrative reforms and Public Grievances (DARPG). Guidelines address the entire lifecycle of a Portal / Mobile App, web portal/application right from its conceptualisation to design, development, maintenance and management. KSCMA (Mobile Web) should comply with these guidelines.

Optimized Application Start-up Time

User experience is heavily influenced by the initial start-up time of an application. Offline Web application technologies like HTML5 AppCache [HTML5-OFFLINE] bring Web applications into parity with native applications in terms of their start-up time and their ability to be used even where network coverage is intermittent. The following techniques to help minimize application start time should be considered:

- Use Offline Technology
- Consider Partitioning Large Scripts
- Use Local Storage

- Minimize Number of Local Storage Queries

Minimize perceived time

Lowering perceived latency is an important factor in improving the overall usability of an application. A number of techniques can be used to lower perceived latency:

- Enable Incremental Rendering
- Keep the User Informed of Activity
- Avoid Page Reloads
- Preload Probable Next Views

Design for Multiple Interaction Methods

Interaction methods vary across devices. Three main interaction methods should be considered when designing the UI:

- Focus Based: The browser focus "jumps" from element to element;
- Pointer Based: Key-based navigation controls a pointer that can cover any part of the screen;
- Touch Based: Events are related directly to a finger or stylus touch position on the screen.

The optimum configuration of UI elements varies depending on the interaction method used by the device. Ideally, the UI should be adapted based on knowledge of the interaction methods supported by the target device. If this is not possible, then the UI should be designed to provide a good experience for each of these different interaction methods.

Preserve Focus on Dynamic Page Updates

The JavaScript focus method can be used to move the focus to the part of a page that has changed. However, if unexpected, this can confuse or irritate the user, especially if returning to the previous focus is not easy.

Use Fragment IDs to Drive Application

View Applications can switch views without a full page reload by showing and hiding sections of content. However, this means that the browser button doesn't work by default, and it is not possible

to link directly to specific views within an application. Usability is enhanced by enabling both of these features:

- Enabling deep links (e.g. to the content of a specific email) means the user can bookmark this view and return to it quickly;
- Enabling the browser history provides a natural method to navigate application views that is natively supported by the browser.

Make Telephone Numbers "Click-to-Call"

Standardized URI schemes have been defined for some common device functions, e.g. making phone calls, sending an SMS, and managing address books. These URI schemes, if supported, can enable users to easily use these functions from applications.

Ensure Paragraph Text Flows

On small screens it is important that paragraph text flows both so that it doesn't require horizontal scrolling and so that it will re-flow if the view orientation is changed.

Ensure Consistency

Devices User credentials valid on one device should be valid on other devices. User preferences captured on one device should be accessible on other devices. Data updated on one device should be viewable consistently on other devices. An important example of this is offering a consistent experience where data entered on a desktop is available on a mobile and vice versa.

Consider Mobile Specific Technologies for Initiating Applications

Network-initiated content delivery ("push") methods allow notifications and updates to be sent to the user even when they are outside of the application context.

Use Meta Viewport Element to Identify Desired Screen Size

Certain classes of browser attempt to display desktop pages on a small screen by automatically zooming the display. This can be problematic for applications that have already been optimized for a small screen. The viewport meta tag tells the device at what scale to render the page.

User Profile

The KSCMA platform should maintain citizen profile in a secure manner. The profile will have sections for storing citizen personal details, preferences and data required to access department services without having to re-enter every time.

A onetime user registration page should be provided on App and Mobile web so that information can be collected and edited at a later date by the citizen. Profile Manager should have at least the following features:

- Save user registration details and support edit/update of these details
- Pre-population of user data wherever required in the service work flow. For example, once user has registered himself/herself, he/she need not enter his name, address etc. in an particular application or form filling.
- Language setting can be done in profile manager so that the user need not opt for his preferred language each time he uses the services.
- Store specific parameters that can be pre-populated when accessing specific departments. For example, in electricity department the user address, connection number can be stored in the profile so that these can be populated in the API call to the department. The user should also have an option to modify these parameters.

  By sourcing user data from different sources, identifying newer target segments, discovering hidden patterns and profiling citizens' behaviour, government departments can usher themselves into unique data driven user management environment. They can then leverage citizen centric user data as a strategic asset to:

  - Develop a 360° view of citizens
  - Personalizing content and service delivery
  - Slicing and dicing consumer data to identify user segments to target

Service Channels

The KSCMA platform should support services enablement over the following mobile channels and interfaces:

Smart Client App

Smart client app should be enabled on Android, iOS, Windows or any other platform as required. The features in the Mobile portal should closely match the features in the mobile app and integrate with the same API integration layer of KSCMA.

Following are some of the features that should be enabled through the KSCMA:

- The app should provide quick and responsive experience even with limited bandwidth and pages as required should be locally cached on the device.
- It should work on both online and offline mode wherever the pages are locally cached. It would need connectivity only when it requires calling an API. Further, it has to be ensured that the cached data is not exposed to any 3rd party in any form.
- It should work on all Android, iOS and Windows devices with the versions of operating systems released by them in last three years from the date of work order and all future releases.
- The App should support security features such as mobile OWASP and should pass security testing by a third party.
- It should support device elements such as accelerometers for enabling apps which works on motion/shaking. Example: Women safety app and other emergency services which can trigger notification based on shaking the device.
- It should be able to use the device features to capture data like Images, Bar-codes, Audio, Videos, GPS, Document pages along with date and time stamping and be able to sync these to the server.
- It should also allow to upload stored data from the device like media files (image, audio, video), PDF etc.
- It should have search functionality across all the pages.

Mobile Web

Mobile Web portal should support all device form factors like mobile, tablet, desktop etc. through a responsive screen. It should be Operating System and device agnostic. Following should be the features supported by Mobile Web:

- It should work on all mobile and tablet form factors by recognizing the device details automatically.

- It should be OS agnostic (at least all standard OS like iOS, Android, Blackberry, and Windows)
- It should work on all standard browsers like IE, Chrome, Safari, Firefox etc.
- Support for dial to call feature from a page.
- It should support multiple languages as specified in section 5.1.8.
- It should be possible to make on-the-fly changes to the portal through a UI and immediately make these available to citizens.
- The user experience of the citizen on the Mobile Portal and App should be similar in terms of look and feel, navigation, menu and access to preferences and other data.
- It should have search functionality across all the pages.

Low bandwidth support

A mobile portal as well as apps should be able to provide services at low bandwidths also. For this, the mobile app and portals should be tuned for low bandwidths to facilitate access of services by users when bandwidth is low.

Pull SMS

In Pull SMS services, citizen sends an SMS to a short/long code along with a keyword and text which will be routed to a configured service. The service can send back a response through the same short code/long code as per the service logic. This type of service is mainly used for informational service where the citizen wishes to track or obtain information. The syntax for the service will be made available through a help menu or as response, if the citizen sends a wrong format request. Validation of the request sent by the citizen shall be done by the service business logic. Pull SMS services can be of 2 types:

- One way pull SMS: Here the citizen uses to either capture data or report any event. Example: citizen provides his feedback on SMS
- Two way or transactional Pull SMS services: Here the citizen goes through series of interaction through pre-defined syntaxes to either seek information and/or do a payment transaction.

Push SMS

KSCMA should provide interfaces to departments and authorized users to send SMS messages to citizens. Though push SMS service is envisaged for transactional service however, it should support both transactional and promotional Push SMS services. It should support sender ID for required departments as per the TRAI guidelines. It should support following ways of Push SMS services:

- API based: KSCMA should provide a standard API to the Departments to avail SMS services and support text, binary and Unicode messages. ii. Bulk Push through UI:
- KSCMA should provide a user interface to the Departments to add messages and user mobile numbers to push any bulk SMS. This should be possible through file upload as well as FTP access to files. This should allow scheduling the messages as well as replacement of parameters so that customization is possible.

IVR (both Inbound and Outbound)

This Module shall support building Interactive Voice Response call flows that can be linked to both Inbound and Outbound calls. When a call lands on to the configured numbers or extensions, the IVR system should use both the called party and calling party numbers and allow the calling citizen to navigate the configured services using key press (DTMF) with cut through facility during announcements.

It should also be possible for the system to use preferences of the citizen in terms of language as well as other data to make it simpler to access and utilize the services. The calling party number should be used as the citizen identity and allow service related data to be retrieved and used so that the citizen need not enter data again. It should be possible through a graphical interface to be able to add new flows/modify existing flows/ change prompts and publish these immediately without having the take the services down.

The KSCMA platform should generate extensive logs that will track the user navigation and the options selected for audit purposes.

The IVR application shall integrate with the common API integration layer for any department service interaction and shall support integration with other message channels such as SMS to allow messaging through those channels.

The Outbound Dialer System shall be able to initiate calls to the list of mobile numbers that can be configured by any department. It shall be possible for the department to specify a prompt as

well as a call flow either through the Application Call flow UI or through VML. An API shall also be provided so that departments can initiate Voice call to a number with linked prompt or call flow that has been configured on the system.

Reporting should be provided that indicates the number of successful calls, failures with reasons as well as the menu traffic for a given period.

Call Centre for handling IVR queries

Partner Agency has to manage the Call centre for voice calls. All the expenses, except charges for PRI line, in running the call centre operations shall be borne by the Partner Agency.

Support Ticket System

The support ticket system shall take incoming user requests for support and automatically generate a customer service ticket which shall be mailed to them instantly. In further communication related to the issue same ticket number shall be used and once the request is resolved the ticket shall be closed.

Ticket system shall act as a shared inbox for all customers' questions and concerns, no matter what channel the customer uses to contact the portal support team—email, chat, Twitter, etc., the support agent shall be provided with an easy to use ticket management system to make it much easier for the agent to help the customer solve the issue more quickly to their satisfaction. Manpower shall be proposed for handling the support ticket system.

Support Over Social Media Channels

Social media is an effective medium of support system and grievance redressal. Solution shall be integrated with the all major social media platforms. All important stakeholders and service providers shall be connected to the social media platforms. There shall be a system in place through which support system workflow can be managed.

Live Chat

Solution must have provision for Live Chat with visitors on the portal in real-time, capture the queries, and continue conversations by email if they leave. Resources shall be deployed for the live chat support. It should be available 24x7 initially in English & Hindi only.

Annual Maintenance

The annual maintenance for a period of 5 years will be applicable on all the services from the date of go live.

Roles and Responsibilities of the selected Agency

The following section outlines the responsibilities of Varanasi Government, Selected Agency and Integrating Service Providers.

Selected Agency

- The Partner Agency is responsible for designing, development and maintenance of the KSCMA platform as mentioned in the above document and to comply with all necessary standards and regulations.
- Responsible for integration with SMS Aggregator for SMS based Push & Pull services.
- The Partner Agency shall provide multi lingual support as mentioned in section 4.8
- KSCMA platform will be hosted on DC and DR site in the NIC cloud or any other DeitY empanelled cloud service provider on hot stand by mode so that in case of a failure at DC the operations of KSCMA platform shift to DR site without affecting the availability of platform.
- Responsible for day to day operation of the KSCMA platform including reporting, issue resolution etc. pertaining to the KSCMA platform.
- Responsible for creating APIs for department for enablement on KSCMA platform.
- Responsible for creation of APIs for external entities/third parties.
- Documentation and publishing of integration APIs on the KSCMA web portal.
- Compliance & Certifications
- Responsible for compliance of the platform to various guidelines & regulations (eg. RBI's mobile banking & payment guideline, TRAI's Bulk SMS Guideline).
- Provide necessary help to Varanasi Government for various certifications which are mandatory for smooth functioning of KSCMA.
    a. Varanasi Govt. will pay for the certification cost (eg. PCI / DSS).

b. Varanasi Govt. to decide on the timing for the certification depending on the business need.

- The Partner Agency will create and take a sign-off on the documents required at various stages of SDLC including FRS (Functional Requirement Specification) during KSCMA development and maintenance and support. It will be also responsible for regular updation of the documents as and when required.
- Conduct training to help government departments to enable mobile services for the respective departments so as to generate maximum benefit out of the mobile governance initiative.
- Will undertake all the tasks related to hosting, deployment and operation for smooth functioning of KSCMA platform on NIC Cloud or any other DeitY empanelled cloud service provider, with due permission from Varanasi Govt..
- Partner Agency will be responsible for procuring all the necessary hardware and software for deployment and running of KSCMA project.
- Will provide all the information related to network infrastructure, internet connectivity, power backups for smooth functioning of the KSCMA platform on NIC Cloud.
- Provide backup tapes/disks for periodic backup of the data, software and other related configurations of KSCMA platform in DC and DR.
- Responsible for providing Level 1 support:

    - Publish a number for citizen to dial-in to lodge help desk request.
    - Publish email id for citizen to send request via email
    - Help Desk personnel should be familiar with English, Hindi and all Indian Regional Languages.
    - Help Desk should be available 24x7 from 8:00 AM to 8:00 PM.

- Work closely with Varanasi Govt. to manage day to day relationship with telecom operator, financial institutions, other government departments and any other external entity as identified by Varanasi Govt. for operationalization and management of the platform.
- Appoint Payment Gateway and Banking partners for all Payment services like Netbanking, Credit cards, Debit cards, IMPS, Telco Wallets etc..
- Liaison with Payment Gateway and Banking partners and manage all necessary day to day coordination with them.
- Manage FAT (Functional Acceptance Testing), Load Testing, Performance Scalability Testing. The Partner Agency will be providing the necessary baseline documents and other documentary evidence of carrying out the testing for KSCMA project.

- Will be responsible for getting all necessary sign offs and approvals from Government Departments.
- The Partner Agency is allowed to sub-contract the work pertaining to Application Enablement task ONLY to other agencies. No other work shall be allowed to be sub-contracted. In cases where the work is sub-contracted, the liability of SLAs would be with the Partner Agency

Implementation Strategy

The below table highlights different stages of the portal and mobile application. The agency/bidder is expected to follow the stages for seamless implementation of the project.

Stage	Deliverable	Activities to be done by the Agency
Requirement Gathering	Final brief document	Initial brief/ Client meeting
		Agency sends a questionnaire for gathering insights, problems & expectations.
		Brief document (initial brief + insights from the questionnaire)
		Client sign off on the brief document
	Varanasi Portal / Mobile App/App	Development Brand guidelines
		Development of Fonts
		Development of Logo
		Development of Iconography style
		Any specific guidelines to be followed by the Agency shall be shared with the department
		Process & Credentials for procuring Images
		Process & Credentials for procuring videos
		Raw content for the Portal / Mobile App
	SRS (Tech requirement details)	Provision of Domain Name to be acquired by the department.
		Server Details (Application & Database) - Test Server (Windows / Open Source & SQL details) + the configuration of the test server should be the same as the Live Server

		Application Security (Appsec) + Vulnerability Testing Guidelines
		List of Portal / Mobile App Compatibility List - Devices, Browsers, Resolutions
		List of Portal / Mobile App Functionalities
		Any other details required from the tech side in terms of support from the Data Centre shall be identified at this stage
Project Strategy	Concept	Brief document
	Portal / Mobile App Sitemap/Product document/User Journey	Client sign off on the sitemap / product document / user journey
		Site Map / Product Document / User Journey
Navigation/User Experience	Final portal, mobile app wireframes	Raw Content
		Content Structure - Mapping the content against the sitemap
		Portal / Mobile App Wireframes
		Client signoff on the wireframes
		Portal / Mobile App Sitemap / Product document / User Journey
Portal / Mobile App Content	Communication Strategy and placement of portal and app content	Portal / Mobile App Wireframes
		Placement of Raw content
		Client sign off on the final content
	Title, Meta Tags & Description + Alt Tags for all Media - Images, Videos etc.	Client sign off on the final content Wireframes
	Share copy - Facebook	
	Share copy - Twitter	

	Share copy - LinkedIn		
	Share copy - WhatsApp		
Portal / Mobile App Development Initiation	Portal / Mobile App structure / Architecture / Database design	Server details	
		SQL Details	
		List of Portal / Mobile App functionalities	
	Backend Fuctionality	Admin panel functionality document	
		Image for share functionality	
	Share Fuctionality	Content for share functionality	
		Brand guidelines	
Visual Design	Mood Board	Placements of Fonts	
	Look and Feel	Placement of Logo	
	Desktop and Mobile UI	Implementation Iconography style	
	UI Kit	Image Procurement guidelines	
	Designs	Video Procurement guidelines	
	Social media share images	Wireframes to be converted into final screens	
	Motion Tests	Finalisation on the workflow of the application	
Portal / Mobile App Developmen	Front end, Back end & Integration	Integration of visual design and the workflow of Portal / Mobile App pages	
		PSDs - Desktop + Mobile + Tablet (Potrait/Landscape)	
		Integration of the approved fonts, Images, Icons, Tiles, Tags, Description, of the portal and mobile app.	
Security and Testing	Testing		Social Media share copy & images
			List of browsers, resolutions & devices.
			List of browsers, resolutions & devices.
			Content check
			Functionality testing
			Interaction testing
			User acceptance Testing

			Broken links if any
			Compatibility testing on browsers & devices.
			Load testing
	Security		Appsec Document + Vulnerability Testing Guidelines
Portal / Mobile App Deployment	Portal / Mobile App Deployment		Approval from the client on the Portal / Mobile App
			Final server details
			Domain Pointing
			Final check content, functionalities, broken links & compatibility across all devices
Handover	Final source files		Admin panel functionality document
	Handover Document		
	Admin panel training		

Final testing and certification

The Project shall be governed by the mechanism of final acceptance testing (User Acceptance, STQC) and certification to be put into place by the VSCL, guided by the following principles:

- VSCL reserves the right to nominate a technically competent agency ("Final Testing and Certification Agency") for conducting final acceptance testing and certification;
- Such Final Testing and Certification Agency will lay down a set of guidelines following internationally accepted norms and standards for testing and certification for all aspects of project development and implementation covering software, hardware and networking including the processes relating to the design of solution architecture, design of systems and sub- systems, coding, testing, business process description, documentation, version control, change management, security, service oriented architecture, performance in relation to compliance with

SLA metrics, interoperability, scalability, availability and compliance with all the technical and functional requirements of the RFP and this Agreement;

- The Final Testing and Certification Agency will be involved with Project from the development stage to ensure that the guidelines are being followed and to avoid large scale modifications pursuant to testing done after the application is fully developed;
- The Final Testing and Certification Agency may engage professional organizations for conducting specific tests on the software, hardware, networking, security and all other aspects;
- The Final Testing and Certification Agency will establish appropriate processes for notifying the Partner Agency of any deviations from the norms, standards or guidelines at the earliest instance after taking cognizance of the same to enable the Partner Agency to take corrective action;
- Such an involvement of and guidance by the Final Testing and Certification Agency shall not, however, absolve the Partner Agency of the fundamental responsibility of designing, customizing/ developing, installing, testing and commissioning the various components of the Project to deliver the services in perfect conformity with this Agreement
- Vendor has to facilitate User acceptance testing environment for VSCL.
- A security Audit (STQC) of Complete Application to be done by the vendor before moving into production environment

The Mobile App should use Varanasi GIS Maps & Smart elements. User should have an option to download the map of Varanasi for the first time and should have option in the settings to check the download option.

B. Shri Kashi Vishwanath Temple (SKVT)- Web site, Queue Management and Live Darshan

a. Queue Management System (QMS):

Comprehensive Queue management system by the way of registration of Pilgrims by capturing the data, finger/photo, allocate the time slot for Darshan issue the card/perchi, while allowing pilgrim for Darshan verification need to be done and must be operational 24x7 basis.

The software which works on LAN/WAN in online/offline mode in integrated manner and must have features like:

- time slot wise number of registrations,
- must exclude the times of Aarties,
- must incorporate Darshana of lord from inside and out side of center sanctum of temple,
- must work in integrated manner,
- there must be proper checking system,
- must be able to stop fraudulent practices,
- must meet the peak hours and ideal hours requirements,
- must ensure to complete the Darshana within stipulated time printed on the tickets,
- easy record keeping and retrieval system,
- the access card be printed with reporting time/date/and gate no. for darshana, and card should not print without capturing photograph of devotees/pilgrims
- token for booking langar/prasadalay should be merged with the QMS to avoid queues and the devotee must be able to redeem the token at free of cost
- easy access and quick disposal mechanism on queue verification counter,
- must capable to capture devotees/pilgrims data finger/photo and allocate the slot for Darshana,
- available Access Cards to the devotees/pilgrims at free of cost,
- must be capable of track record of the missing person in real time and report should be generate within a minute and just the touch of the finger his name should remove from missing person list,
- must be capable to centralized registration of devotees/pilgrims,
- must be capable with 20 barcode/QR code technology,
- must be capable to prepare emergency response plan,
- must me capable to search pilgrim name wise and token number-wise,
- must be capable to manage any delay happens due to unforeseen situation,
- must be capable to manage let coming devotees/pilgrims
- must maintain the DR system and any failure shall be managed within a minute time.
- must be capable of printing priority access cards
- works on LAN and VPN,
- the software must be capable to show real time data that how many devotees/pilgrims are inside of the temple exist based on a particular time how many access cards issue minus how many devotees/pilgrims exit from the exit gates, and this data should be available on the display

boards as well as VSCL control room and hourly report send to temple administrator as well as police station.

- the software must be capable to keep record of different hall as well as its capacity, as soon as the devotees/pilgrims capacity increases to hall the capacity he has to inform to the devotees/pilgrims through SMS or announcement about the place where he has to wait and how much time they have to wait.
- the software must compatible to capture the biometric records of devotees/pilgrims but this option should be optional, only used when it will needed.
- all the reports and access cards shall be print in local languages as well as in English
- various report like:

  i. day wise and time slot wise devotees/pilgrims visited O Missing Persons and his track record
  ii. system should have ability to provide periodic MIS reports
  iii. daily Location wise issued cards count, O Hourly pilgrims count,
  iv. hourly Token issues report and Hourly Token Verification Report,
  v. hourly SMS of Location wise pilgrim registered/ Card issued and verified at check point.

The development of the above audited portal from day one and its operation and maintenance till the entire contact period will be responsibility of the bidder. The bidder must maintain the Change Management mechanism for updation required time to time. The bidder used the licensed copy of all software used for this purposes.

The Access Card must be of:

- multi color,
- max 6x4 inches in size
- 250 GSM thickness,
- barcoded,
- validity of card 6 hrs
- issue date and time must be in dd/mm/yyyy hh:mm:ss format,
- multi color advertisement of sponsor (only public interest message approved by VSCL) can be printed on back side of the Card maximum 1 advertisement on the back side of the ticket,
- the advertisement shall be only Government Schemes and Social messages related,
- the devotees/pilgrims are allow to keep access card after verification.

Backup Plan – The bidder must plan complete backup strategy and enclosed it with the bidder document to ensure the data backup and handed over the complete backup to the VSCL at the end of the contact.

Storage – The bidder must keep real-time storage of complete data, photos and videos of all the cameras installed at the counters for various purposes.

Surveillance Cameras – The bidder must install cameras along with licensed surveillance software `at all the counters and the real-time feed of all the cameras shall be given to VSCL control

Room and keep the cameras recording for future use along with the retrieval process.

Network Plan – The bidder plan the network and installed the networking equipment at each counters which are accessible from LAN or WAN to all the counters as well as VSCL control room.

Display Units - at lead 10 Big led display units size not less than 3x4 feet which display real-time data of devotees/pilgrims are inside of the temple through queue management software the calculation shall be based on a particular time how many access cards issued minus how many devotees/pilgrims exit from the exit gates of the temple.

Civil works/ counters erecting/ electrical points/power backup /furniture & other amenities Communication/ LAN/ OFC/ Internet /rent of place if counter is other than VSCL premises/ power charges etc. bidder shall bear the complete cost and should not charge anything from VSCL.

Compatible Hardware / Systems with licensed OS and Application Software(s) / Servers with licensed OS and Application Software(s) / Clients with licensed OS and Application Software(s) / Printers/ Licensed Software/ Manpower/ Consumables, bidder shall bear the cost of these items and should not charge anything from VSCL. AMC of all the equipments installed at the counter required strictly and cost of AMC will be bear by the bidder only.

The bidder erects minimum 15 counters on public places and 10 counters at temple premises.

b. Installation of variable sign boards and direction boards for SKVT

Design

The SKVT is looking for sign designs for primary destination wayfinding signs. The design of these signs must be durable, adaptable, reflective and meet the SKVT minimum requirements. Bidder must provide a minimum of one sign design for each category. All sign designs must incorporate the SKVT logo. Sign designs should be adaptable and updateable.

Fabrication Types and Quantities Required

As per the Way finding Plan the following quantities of signs shall be provided by the vendor:

- Primary Way to Enter Temple Directional Signs
- Way to Exit Directional Signs
- Way to Kitchen Directional Signs
- Way to Toilet Directional Signs

Primary Way to Enter Directional Signs - Primary directional signage is to be located in and around the temple for guiding the way to enter the temple and to avoid the rush. These signs are scaled to be easily identified by vehicle or walking pedestrian. They should also create an entrance to the destination.

Way to Exit Directional Signs - Way to Exit signage indicates the route to find the way to exit the temple.

Way to Kitchen Directional Signs – Way to Kitchen directional signage will be smaller versions of the primary directional signage. This will help the devotees find the way to the kitchen.

Way to Toilet Directional Signs - Secondary directional signage is to be smaller versions of the primary directional signage. This will help the devotees find the way to the toilet.

Performance Requirements-

- Provide workmanship and materials, free of defects. Defects shall be defined as, but shall not be limited to delamination, abnormal deterioration, fading and discoloration, weathering, failure of

securing to substrates indicated, cracking, corrosion or coating damage, or visible scratches on surfaces.

- Signage shall not bear manufacturer's code or other identifying marks on any area or part, which may be visible in the normal positioning, attitude, or use of the sign item. Date stickers to be affixed to back of signs.

- Selected vendor shall ensure that the design of support substrates and structures are adequate and compatible for the performance of all work required.

- Submittals:

    - All vendors shall submit a minimum of one design for each type of sign as identified above. Vendors shall provide a PDF of each design and three (3) 11"x17" copies after bid selection.
    - Prior to commencement of work, selected vendor shall provide PDF's and three (3) 11"x17" copies of shop drawings of all fabricated items. At a minimum, these drawings shall include:

        a. Dimensions, details of construction, materials, technical data, and installation instructions for each type of sign required.
        b. Anchorages and accessory items.
        c. Location template drawings for items supported or anchored to permanent construction.

- Selected vendor shall submit samples and color match samples (colors and finishes as indicated on drawings) for each sign type.

    a. Submit proofs of artwork, map art, and symbols.
    b. Submit prototype samples and color match samples.
    c. For all sign types, submit complete alphabet numerals, punctuation, materials, and graphics for review prior to start of fabrication. If more than one supplier's cut will be used, submit each cut for review.
    d. Submit templates or samples showing front or word spacing for each dimensional wall-mounted letter, for review and written approval.

- Selected vendor shall provide structural drawings, with engineer's signature and seal, for all sign types included in the project identifying all applicable mounting applications.

- Materials:

  Materials shall be new stock, free from defects impairing strength, durability, or appearance.

  - Aluminum:

    - Aluminum used for all exposed surfaces shall be a minimum thickness of with a painted finish as selected by Designer. Aluminum sheet thicknesses shall be as noted on plans.

    - Aluminum used for concealing framing of signage shall be a minimum thickness of with a mill finish.

    - Selected vendor shall provide aluminum of the best commercial quality with the various form straight and true. Selected vendor shall replace materials that have scratches, scars, creases or buckles.

  - Fasteners shall be non-corrosive type fasteners, nonconductive or insulated when joining non-compatible materials.

  - Other proposed sign materials must be pre-approved by the SKVT prior to the installation. Vendors must provide cut sheets for the proposed material to be approved by the SKVT.

- **Warranty**

  Selected vendor shall provide a five (5) year written warranty on all materials and workmanship for variable sign structures.

- **Preparation for Installation**

  Selected vendor shall provide adequate temporary support to assure the structural value and integrity of the affected portion of the work during storage outside prior to installation by others.

c. Live streaming of the Darshan of Shri Kashi Vishwanath at display boards

- Rights of Live Darshana of Shri Kashi Vishwanath 24x7 basis for entire agreement period. To perform the task cost of appropriate Hardware, Software, Internet connectivity, power backup, manpower, installation, testing and Maintenance will be born by proposer.

- Separate agreement shall be made for each platforms like Cable & Dish TV, Mobile (iOS, Android, Windows), WebSite/Portal and outdoor LED display units (min. size 70") for 3 locations within the temple and 7 outside the temple premises.

- The Live Darshan of Lord Shri Kashi Vishwanath on SKVT official web portal and official mobile app shall be available Free of Cost for all the Devotees.

- For LED Display units approved advertisement from the SKVT for donations will be allowed.

- Safety of all the equipment used for the above used in the temple premises or outside of the premises shall be sole responsibility of proposer.

d. Installation of Public Announcement Systems to manage the rush

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

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

- Public Address system shall be used at those critical locations within the temple area 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 MSI shall describe in detail the design, operational and physical requirements of the proposed public announcement system to demonstrate compliance with the specified requirements of RFP.

- 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.

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

e. Revamping the look and the content of the website

The scope of work includes planning, requirement-gathering, design, development and testing, delivering and migrating existing site to the new portal. It also includes regular maintenance and updating of the website for next 5 years. SKVT expects that the portal and mobile apps will be delivered on "turn-key-basis".
Details of various elements of the scope of work are as follows:

Information Content:

- The portal will be superset of the existing website

- In addition, the portal should provide appropriate plug-ins to passively/actively integrate the Portal with Kashi tourism website and app.

- The portal should be regularly updated with thematic content based on Shri Kashi Vishwanath's social and devotional initiatives. The content should be optimized for social media in text and multimedia format.

Other Required Features

- The portal and mobile app should accompany a comprehensive content management system to support a variety of users ranging from devotee to Management. It should allow the administrator to creates user roles and allow the setting up of access rights ranging from entire site to a specific page.

- It should provide for flexibility to modify the design when a major event has to be published.

- Design should be flexible to accommodate new pages.

- Design should allow changing the interface templates for fresh new look as and when required.

- The portal should be based on International standards.

- It should be compatible to various browsers including IE, Mozilla Firefox, Chrome, Opera etc. mobile app should compatible to all devices/OS

- It should provide secure integration with various payment gateway for online payment transactions involved in processes such as online Donation, Membership etc.

- The Web portal and Mobile app should allow users to share their views, feedback, solutions and suggestions online through the webmaster, and also allow podcasts, webcasts and other wikis and forums.

- It should provide a search module for efficient information retrieval.

- The portal should have a direct mailing facility where mails could be sent to different contact persons.

- The website should incorporate necessary security features against hacking and defacement.

- All logins and payments transaction must operate on secure protocols. It should provide support for website security audit.

- The portal should comply fully with the guidelines issued from time to time by the Government of India and the Government of Uttar Pradesh for development of websites.

- The portal should be user friendly, and should allow for features such as voice enabling and enhancement of font size.

- Web portal and Mobile apps should able to display Live Darshan on all the platforms. Security of live darshan link should be maintained .

- The Devotee should be able to book langar/prasadalay through the app/portal and should be able to redeem his token for free.

- RTI, Board Resolution, published books should be displayed in e-book format with bookmark facility.

Technology:

The entire portal and mobile app should be based on latest technology Open source freeware or license Software.

Development Methodology:

The development methodology should follow an iterative-prototype approach especially during early design phase.

Hosting:

- The vendor may either host at its premises or can use a third party to provide hosting services. However, it should be ensured that the party is competent enough to safeguard trust Web portal

and provide robust security to maintain the site integrity and confidentiality. The other features which trust would prefer to have in the host ISP are:

- Be highly reliable with at least 99.5% service up time.
- Have been providing their services for at least five years.
- Have adequate Disaster Recovery facilities
- Ensure that security patches are regularly installed in their software and provide proactive defense against malware and other cyber attacks
- Provides Secure Sockets Layer (SSL) encryption during payment transaction and user login.
- Pro-actively monitor and maintain services to maximum server performance and up time.
- Only allow legal files.
- Provide clear and proper billing.
- Safeguard privacy by not sharing, renting or selling its information.
- Promptly inform trust about any changes to the T&C and/or their plan.

SKVT reserves the right to host the Portal or any other server. In such a case, the vendor will be required to provide all other services as mentioned in this document on the server as chosen by Trust.

Website features:

This website will enable external users to obtain information on:

- The Trust.
- The temple.
- Trust Management.
- Trust Administration.

- Social Services by trust.
- Publication
- Prasadalay.
- News and events.
- Live Darshan
- Daily aatries and other function photo.
- Any other information deemed necessary from time to time.

It will allow internal users (Management, Administration, staff) to view all of the above, and also view and access:

- Trust circulars, notifications and guidelines
- Calendar of events/Functions
- PF Statement.
- Seniority List.
- Donor/Charity List
- Any other information necessary from time to time.

Design and Layout:

Being the trust impart services to devotees, the website should have an elegant design with proper background, light colours, a neat, uncluttered look and a user-friendly, easy-to-navigate layout.

Language Support:

Web portal and Mobile apps should support multilingual. English, Hindi, Sanskrit are required languages. Technology used for development must support all these languages.

Audio Guide:

There are various historical locations in Temple premises. Information of each location (Audio/Video) must be incorporated in website as well as mobile application.

e-Mails:

Bidder has to give proper solution for emails like Exchange Server or google interface service.

Data entry Forms:

- **Temple Registration Form:**
  Various suppliers should able to register themselves with SKVT.

- **Aarti Registration Form:**
  Detail database of aartis to be maintained.

- **Feedback Form:**
  Feedback of devotees for various services need to gather, it should be multilingual.

- **Reports:**
  Reports of above data entry in specified format by SKVT, with export facility.

- **Other:**
  Trust will give the forms as and when required.

- **Online promotion of the website to increase donation to the temple**
  a. Formulating and implementing an online campaign strategy for the promotion of the SKVT Website to increase donations.
  b. Creating SKVT resonance, connecting and engaging with the influencers using Google, Facebook, Twitter and YouTube.
  c. Providing amplification of Digital Marketing communication & messaging through planning and execution of a Digital Marketing activity across both Paid Media and Non-Paid media avenues on Digital and Mobile for Campaign (s), in consultation with SKVT.
  d. Theme based messaging will need to be developed by agency which will include but will not be limited to powerful, engaging and impactful messaging, taglines and hashtags etc. Raw content will be provided by SKVT.
  e. Online campaign will include Live Twitter (Periscope), Twitter Trending and Live Facebook sessions.
  f. Design, development and adaptation of creative material units which will include but will not be limited to web banners, graphical advertisements, GIF, PowerPoint presentations, animation material, infographics, html e-mailers, creative material for social media engagement activities such as quiz, contest, trivia etc. Production of videos will be out of the scope of this RFP. Adaptation of provided material

including videos, in various format/renditions will be done by the agency. Raw content and videos will be provided by SKVT.

g. Applicants need to ascertain and ensure the availability of adequate man power to deliver 24/7 services.
h. Planning and executing a "Social Media Monitoring Program" on Digital platforms.
i. Projection for Ad impressions, Website hits, Facebook Likes and Twitter Followers must be provided with technical proposal.
j.

f. Integration with SMS Gateway

SKVT requires Short Messaging Service (SMS) Solution to be hosted by the service provider to generate SMS for SKVT devotees for service related messages etc.

- Any Integration required for providing this facility will have to be done by the service provider.
- The bidder shall be procuring the number from the Telecom Company for the service.
- The system should support all features based on the following functional blocks:
- Session Management
- Application Management
- Interface Management in form of web portal
- Service Definition Module
- MIS and Reports

The API provided for SMS PUSH/ PULL services shall be used by multiple applications within SKVT. The service provider should have Bulk SMS inbuilt functionalities such as:

a. Multiple Interface Support

b. Bulk Push requirement: bulk SMS sending should be provided through Graphical User Interface (GUI) and API (Application Program Interface).

c. URL Push: One URL should be provided, where the facility to pass the parameters viz. Mobile Number & text/text template would be given. Service provider will provide Bulk SMS connectivity with following protocols:-

- http
- smpp (short message peer to peer protocol)

This connectivity should come with Username and password so that it can be integrated with SKVT applications.

Push Message

The following conditions for Push Message – gateway application Web GUI should also be fulfilled:-

- The application must allow scheduling of messages. There must be configuration options to allow automatic rescheduling of messages that could not sent in a working day.
- The application must be able to support multiple upload formats like CSV, excel, XML and via a Web UI.
- The application must have the ability to create and manage groups. Further, it must be possible to send messages to groups directly without having to enter the individual numbers again.
- The application must support the creation of user defined message templates.
- Application & MIS should open on popular browsers.
- There should be facility for sending SMS to individual numbers or groups. It should also include creating of groups and creating SMS service for each of the groups.

Pull SMS requirement:

- The bidder will use the application link where all queries from the users need to be handed over. After which application will fetch query based data from the database and send to the users using Bulk SMS application.
- The SMS gateway PULL SMS application should be able to decode the request made by the customer, query the SKVT database based on the request and submit back the desired information to the customer over SMS.
- The user initiates the SMS request for pre-defined service logic. User may send the request on long code. Application once received the SMS request, will forward the same to the SKVT over HTTP

or some other given interface for final action. PULL request may trigger an interactive session as well with the application context, if required.

Service Integration:

- Network based Solution: The service provider should provide a WEB based URL. This URL (GUI) should be provided with secure access for sending SMS through SMS gateway to predefined mobile numbers/groups.

- SMS gateway should send back an acknowledgement after delivery on the webpage.

- The application should be able to handle any load.

Group SMS Facility

The Group SMS facility should exist as follows:

- Creation of groups: Groups can be created using web interface. While creating a group logical name can be given to a group and any number of SKVT acquired by the bidder may be added to it.

- Adding the number in Group: Mobile numbers may be deleted or added or modified at any time using the web interface.

- Group SMS: While sending the SMS, selection of the group and to edit the SMS text facility should exist. SMS has to be sent to all the group members. At the same time, same message may be send to multiple groups.

Application

The application should support the following:

- Service provider should be able to send SMS to respective mobile numbers of GSM, CDMA or any other network of any service provider in India.

- Type of interface supported for Individual / BULK SMS: HTTP & SMPP

- Method of providing mobile phone numbers: TXT files with list of mobile numbers or URL based.
- Type of connectivity between SKVT and Service provider: Internet

MIS Reports

- Successful SMS delivery on monthly basis with mobile numbers.
- Mobile number and message list where SMS could not be delivered for each transmission with reason for failure.
- Online web based tools should be provided for MIS reports.
- The application must be able to provide daily and monthly summary reports that show the delivery performance including average time to submit request and successful deliveries.
- Any other default standard reports or any report as desired by SKVT

Following additional conditions should also be fulfilled:-

- The successful bidder has to demonstrate the feature of API GUI & MIS reports before commissioning of SMS Gateway.
- SKVT will not enter into any contract with any telecom service provider. The successful bidder shall be the single point of contact.
- Service provider should be able to send SMS to all GSM/CDMA/3G mobile users in India with sender id "SKVT" or any other id as defined by SKVT
- Type of connectivity between SKVT and Service provider: Internet.
- Check should be properly imposed to avoid Duplicate/ Multiple SMS Delivery to customers.
- The SMS gateway application should allow sending SMSs to subscribers of all service providers in India.

- The SMS gateway PULL SMS application must have security features to ensure confidentiality of sensitive customer data.

- The SMS gateway PULL SMS application should be able to retrieve SMSs sent by devotees to one or more short codes / virtual numbers.

- The SMS gateway PUSH SMS application should be able to send messages at different priority levels. In case the total number of messages to be sent exceeds the capacity promised, messages should be sent first as per higher priority and then following a FIFO rule. Other messages must be en-queued.

- The SMS gateway PUSH SMS application must have the ability to set working hours and working days.

- The Solution should offer configurable mechanism in terms of number of retries & time duration for each retry for messages that could not be delivered immediately.

- Online Mechanism in real time mode has to be provided for SLA enforcement with regard to Uptime of Push /Pull services & Delivery of Push SMS along with flexibility to generate MIS on daily/weekly/fortnightly/monthy/specified date range basis.

- The bidder should integrate with the Dashboard/Website/Portal for Administration features like monitoring of total messages sent within a day/ week/ month, time delay (if any) in sending the messages, no of failed messages (with reasons for failure), invalid mobile numbers, No of Push & Pull Messages sent.

- The successful bidder shall demonstrate the Dashboard functionality & Reports format to SKVT before commissioning of SMS gateway services.

- The bidder shall ensure that SMS whose contents exceeds 160 characters, should be delivered as a single message on receiver's handset.

- The bidder should have proper test infrastructure with capability of end to end testing of all integration with SKVT Applications.

- Check should be properly imposed to avoid Duplicate/ Multiple SMS Delivery to customers.

- The solution should be capable of generating detailed report in Excel/ PDF. The solution should be capable of providing mobile-wise, Date-wise, category-wise reports and aggregated reports per category. The reports should contain timestamps of SMS received at Bidder's server , SMS Sent to the Telecom Operator, actual delivery to the end user & final status of SMS alert along with status description

- It is the responsibility of the bidder to change/ upgrade/ customize its infrastructure / solution at all levels for ensuring the compliance to statutory regulatory guidelines from TRAI etc without any extra cost to SKVT.

- Its bidder responsibility to deliver all SMS to SKVT devotees as per to TRAI guidelines.

Utilities Dashboard

The Utility dashboard should be capable to change behavior of Utility departments in a smarter way and drive incremental, continuous improvements.

The dashboards of different Utility Departments in Varanasi should serve as the front-end interfaces that distill data sets into simple insights using data visualizations.

The Key Utilities include: Water Management Services, Energy and Power Services, Domestic Gas services across the city.

These Reporting dashboards are an analysis tool that allows respective departments to stay in control of their performance of inter departmental or Citizen Centric services.

Types of required reporting dashboards:

- Operational dashboards tell you what is happening now
- Strategic dashboards track key performance indicators
- Analytical dashboards process data to identify trends

An **Operational dashboard** should serve as a reporting tool that will be used to monitor processes that frequently change and to track current performance of key metrics and KPIs of different utilities.

A **strategic dashboard** should serve as a reporting tool to be used to monitor the status of key performance indicators (KPIs), and are typically used by executives. The data behind a strategic dashboard must updates on a recurring basis.

An **analytical dashboard** should serves as a reporting tool that is used to analyze large volumes of data to allow users to investigate trends, predict outcomes, and discover insights.

Reporting dashboards should prove as a smart solution that has the following benefits:

- Foster a culture of continuous improvements
- Data transparency throughout the organization
- Being in control of business decisions by having the right data
- Save time and money on reporting

Improved alignment throughout the organization

4.10 Helpdesk

a. City Operations Helpdesk

MSI shall provide the operational support for all the locations, through a suitable helpdesk system, to ensure that the solution is functioning as intended and that all problems associated with operation are resolved satisfactorily during the contract period. The MSI shall provide a web enabled helpdesk management system with SMS and email based alert system for the Helpdesk Call management and SLA reporting. MSI shall be required to setup a centralized helpdesk at the Integrated Command and Control Center (KICCC).

MSI shall provision for the infrastructure necessary for managing the Help Desk including rent charges for Toll-free telephone line(s) at the Help Desk location. MSI shall provide multiple channels to log a complaint such as Toll-free lines, landlines, helpdesk tool, E-mail, direct walk-in etc. Outage of any component shall be calculated as a time between logging the call and closing the call.

A helpdesk is envisaged to be provided for the resolution of technical queries by internal users. Typical helpdesk activities (indicative) shall include, but not limited to:

1. Deployment of sufficient manpower to attend the helpdesk requests for extending technical support on hardware, network, application etc. to users

2. Deployment of web-based tool for the helpdesk

3. Provide Help Desk facility for agreed SLAs for reporting technical incidents / issues / problems with the system. Help desk facility shall be provided through Toll-free lines, landlines, helpdesk tool, E-mail, direct walk-in etc.

4. Implement a call logging system in line with the severity levels as per the SLAs. The Help desk shall log user calls related to system and assign an incident/ call ID number. Severity shall be assigned to each call as per the SLAs.

5. Track each incident / call to resolution.

6. Escalate the calls, to the appropriate levels, if necessary as per the escalation matrix agreed upon with Competent Authority/authorized entity

7. Analyze the incident / call statistics and provide monthly reports including but not limited to:

    - Type of incidents / calls logged

    - Incidents / calls resolved

    - Incidents / calls open

8. Helpdesk Solution shall further have the capability to upload frequently asked questions and solutions.

Helpdesk becomes the central collection point for service staff contact and control of the problem, change, and service management processes. This includes both incident management and service request management. This shall be the first level of support (L1).

It is also expected that a second level of centralized support (L2) shall also be maintained at the same location from where the various zones/wards can be serviced in case of problem escalation. If a

problem is not resolved by telephone/help desk tool and the User declares the problem to be of an emergency nature, MSI shall dispatch a Field Service Staff member who shall provide On-site Support Service according to service levels given.

The Helpdesk shall act as a single point of contact for all users whether for service requests, incidents or problems. It shall encompass Helpdesk, Asset Management and Vendor Management. In addition, it shall offer a focused approach for delivering integrated Service Management and provide an interface for other functions in IT Services Continuity Management like Maintenance Contracts, Software Licenses etc.

MSI shall implement effective Helpdesk Management procedures to leverage the knowledge gained in providing faster and better solutions, create knowledge bases and prevent recurrence of problems.

Helpdesk Capacity

MSI is required to provide a minimum 8 seater helpdesk at Integrated Command and Control Center (KICCC) during all operation hours as specified in the RFP. However, if the MSI believes that in order to meet the SLAs, additional capacity is required, the same may be provided by the MSI. It is also to be noted any supervisors required for the Helpdesk Operators shall be over and above the minimum operators mentioned above.

Shift Timings

The MSI shall operate the Central Helpdesk for the entire tenure of the Contract as follows:

Category	Shift	Type of Support	Type Support
Helpdesk at Integrated Command and Control Center (ICC) & (Police	Shift 1	On-premises	On-call
	Shift 2	On-premises	On-call
	Shift 3 (Night)	On-premises	On-call
Helpdesk at	Shift 1	On-premises	On-call

Varanasi City	Shift 2	On-premises	On-call
	Shift 3 (Night)	On-Premises	On-call

Helpdesk Operators

The MSI is required to provide Operators at Helpdesk for operating and managing the Helpdesk as specified in this RFP. The Operators shall perform various activities including:

- Understanding the query/issue in the reported request. Query could be related to the following:

- Hardware including issues related to desktop/laptop, printer/multi-function device, local server, routers/switches

- Application including login and password issues, accessing a particular module, navigation assistance, report generation assistance

- Network including internet/intranet and end-user device connectivity

    i. Providing information / clarification on the spot in case of an informational query or providing necessary troubleshooting assistance in case of a logged issue

    ii. In case of technical issues for which a resolution is not possible instantly, the operator shall submit the request into the system for escalation and further action by the MSI's team

    iii. Process all service requests, dispatch them to field personnel who shall perform the follow up

Field Support Staff

The MSI is required to provide Field Support Staff for undertaking all activities on field to complete a call logged by a User. MSI is expected to deploy enough number of Field Support Staff to ensure that SLAs as specified in the RFP are met.

IT / Non IT Infrastructure and application software for Helpdesk

The MSI shall be responsible for procurement, installation, commissioning and operations & maintenance of helpdesk including supply & installation of IT / Non IT infrastructure along with necessary application software (as per indicative BOM) required for the smooth functioning of the Central Helpdesk at both the location

b. Post Implementation Requirements:

Quality Assurance Plan

The Quality Assurance Management process will be implemented by the MSI in a structured and professional manner throughout various stages of the Project. It is intrinsically linked with the provision of safe and reliable systems since the application and control of applicable processes is the fundamental mitigation against systematic error. Achievement of ISO 9000 is the most common metric available to companies and an ISO 9001 compliant design methodology provides a high level of confidence that Quality Management is adequately implemented

System Configuration Management:

The system configuration management activity shall be carried out by the MSI and will comply with the principles depicted in the System Configuration Management Plan.

The MSI shall produce a System Configuration Management Plan to cover change control that occurs during the development phases and at the same time monitor the system configuration.

The System Configuration Management Plan shall address the configuration management in terms of configuration, change control, problem reporting, media control and appropriate configuration management tools.

Reliability Critical Items list should be made. Critical items are defined as System/Subsystem/Component, failures, which result into the highest disruption to service when ranked with other equipment in any system. This ranking will be based on the RAM (reliability, accessibility and manageability) analyses. Ranking severity will be considered for the number of instances, which would delay a service, due to the failure of the equipment. The length of the delay in any smart Varanasi City schedule and the time taken to fix the failure would affect the criticality. The criticality of the item will also be based on the effect of that single item on the entire system.

The assessments include Failure Mode, Effects and Criticality Analysis (FMECA), Interface Hazard Analysis, Quantified Risk Analysis and quantitative analyses. It is recommended that the quantitative analyses be performed using Event Tree Analysis, Fault Tree Analysis or availability simulation modeling:

Class	Types of failures and incidents	Definitions
4	Significant	The failure leads to an incident that requires evacuation or immediate attention to people, while restoration of the operation could take a long time, or lead to a delay greater than 30 min.
3	Major	The failure leads to a disturbance of the operation with a significant loss of missions degrading regularity and "offered service". A delay greater or equal to 3 min but less than 30 min is suffered.
2	Minor	The failure leads to a disturbance of the operation with a delay. A delay greater or equal to 1 min but less than 3 min is suffered.
1	Negligible	The failure has no immediate consequence on the pursuit of the missions but may lead to an intervention in corrective maintenance.

Helpdesk/Contact Centre Solution

Sr. No.	Component	Feature Description

1	**ACD (Automatic Call distribution)**	ACD solution should be highly available with hot standby and seamless failover in case of Main server failure. There should not be any downtime of CC in case of single server failure
		The ACD hardware and software should be from a single OEM and should support VMWare Virtualization for Hardware Optimization.
		The ACD should support active and standby server mode. In case of Main server in the Data center fail the standby server in DR should take over seamlessly. ACD solution should support the placing of Main and Standbyserver in DC and DR respectively.
		The solution should support 50 Agent in one location to start with expandable up to 400 across 4 locations
		The system should support skill-based routing and it should be possible to put all the 400 agents into a single skill group.
		ACD should support routing of incoming calls based upon caller input to menus, real- time queue statistics, time of day, day of week, ANI, dialled number etc.
		ACD should support routing based on longest available agent, Circular agent selection algorithms. Up to 10 levels of customer contacts should be prioritized based upon call or customer data, and calls may be moved within or among queues under workflow control using priority information.
		ACD should support the playing of customizable queuing announcements based upon the skill group that the call is being queued to, including announcements related to the position in queue and expected delay.
		ACD should support Data- driven routing, ACD should have the ability to use data obtained from backend database to make routing decisions. The database can have parameters like a list of holidays, hours of operations, a short list of hot customer accounts, and so on.
		Agents should be able to login, logout, make ready or not ready from the desktop application, Agent desktop should display ANI or DNIS or any customer related data.
		Agent desktop should dynamically pass the call data like ANI/DNI

		any browser based or Microsoft compatible application.
		Agents should be able to chat with other Agents or supervisor from the Agent desktop software
		Agent desktop should support integrated desktop for browser based application.
		Dynamic Re-skilling by Administrator or Supervisor to modify the skills and competencies and agent skills and competencies should be applied immediately
		Supervisor should be able to see the real- time status of agents, supervisors should be able to make agent ready or logout from the supervisor desktop
		Supervisors should be able to barge in a agents call and also if required take a call from an agent and attend it.
		Should support Queuing of calls and playing different prompts depending on the type of call and time in the queue.
		Supervisor to create and configure preview outbound campaigns. The supervisor should be able to specify a daily time range during which outbound calls are made and a set of Queue whose agents make the outbound calls. The supervisor should also be able to specify and import a list of customer contacts to be called.
		ACD should support Web-based administration for addition new agents, assigning skills etc.
2	**Reporting**	Agents should be able to accept, reject, or skip outbound call requests. Agents should also be able to reclassify calls to any one of many call results, such as Busy, Fax, and Answering Machine.
		Users of the Historical Reports should be able to perform the following functions View, print, and save reports. Sort and filter reports Send scheduled reports to a file or to a printer. Export reports in a variety of formats, including PDF, RTF, XML, and CSV.
		Should be able to prepare custom reports using a variety of generally available 3rd party applications that are designed to create reports from databases. Third party applications to have access to the reporting database. Database schema of reporting to be given
		Reporting platform to support custom reports using a combination

		of the Crystal Reports Developer's Toolkit and SQL stored procedures.
		System to provide report of IVR Application Performance Analysis, Call by Call details for all the calls, Traffic analysis reports etc.
		Reporting platform to support Agent level reports, Agent login logout report, report on agent state changes,
		Queue reports, Abandon call reports all the reports should be summary, tabular and detailed report format to be available for the agents.
		Outbound Agent summary or Campaign summary reports should be available.
3	**E-Mail**	Email routing support integration with mails services should be available.
		The administrator should be able to assign one or more email addresses to a single Queue.
		Should support dedicated email agent and Blended voice and email agents
		Agents should be able to automatically resume of e-mail processing on voice disconnect
		Agent should be able to save email draft response and resume at a later time
		Agent should be able to re-queue email.
		Supervisor should be able to access real- time reporting for Agent E-Mail mail volume by Queue
		Supervisor should be able to report Agent E- Mail Inbox Traffic Analysis, Agent email activity Queue wise
4	**IVR**	IVR should Play welcome messages to callers Prompts to press and collect DTMF digits
		IVR should be able to integrate with backend database forself-service.
		GUI based tool to be provided for designing the IVR and ACD call flow.
		IVR should support VoiceXML for ASR, TTS, and DTMF call flows
		IVR should be able to Read data from HTTP and XML Pages

		IVR ports should be twice number of agents

S.No.	Specifications
1	The contact centre solution should be able to route voice/ VOIP calls from centralized Interactive Voice Response System (IVRS) to respective call centre(s) along with interaction history of the calling party.
2	The callers should be able to access the various services through state-of-art centralized integrated Interactive Voice Response System (IVRS). The information is envisaged to be available to the customer through telephone (IVRS) and call centres agents.
3	The IVRS should establish two way communication on the same channel with customers through recorded synthesized voice in Hindi / English / Regional Language or in combination of languages to give information, reply to queries and provide other
4	IVRS should be modular and scalable in nature for easy expansion without requiring any change in the software.
5	It should be possible to access IVRS through any of the access device such as Landline telephone, Mobile phone (GSM as well as CDMA) etc.
6	IVRS should support various means of Alarm indications in case of system failures e.g. Functional error, missing voice message prompt, etc., and shall generate error Logs.
7	The system should have the ability to define business rules based upon which the system should quickly identify, classify and prioritize callers, and using sophisticated routing, to deliver interactions to the best qualified agent in the any of the connected local/remote call centre, regardless of interaction channel
8	The application should provide CTI (Computer-Telephony Integration) services such as: a) Automatic display (screen pop) of information concerning a user/customer on the call agent screen prior to taking the call based on ANI, DNIS or IVR data. b) Synchronized transfer of the data and the call to the call centre agent. c) Transfer of data corresponding to any query raised by any IP agent regarding a query raised by a customer whose call is being attended by the call IP agent. d) Call routing facilities such as business rule based routing, skills-based routing etc.
9	The application should support integration to leading CTI middleware vendors.
10	Should provide pre-integration with industry standard IVR servers and enhance routing & screen-pop by passing forward the information.
11	Should provide facilities for outbound calling list management, and software based predictive or preview dialing.

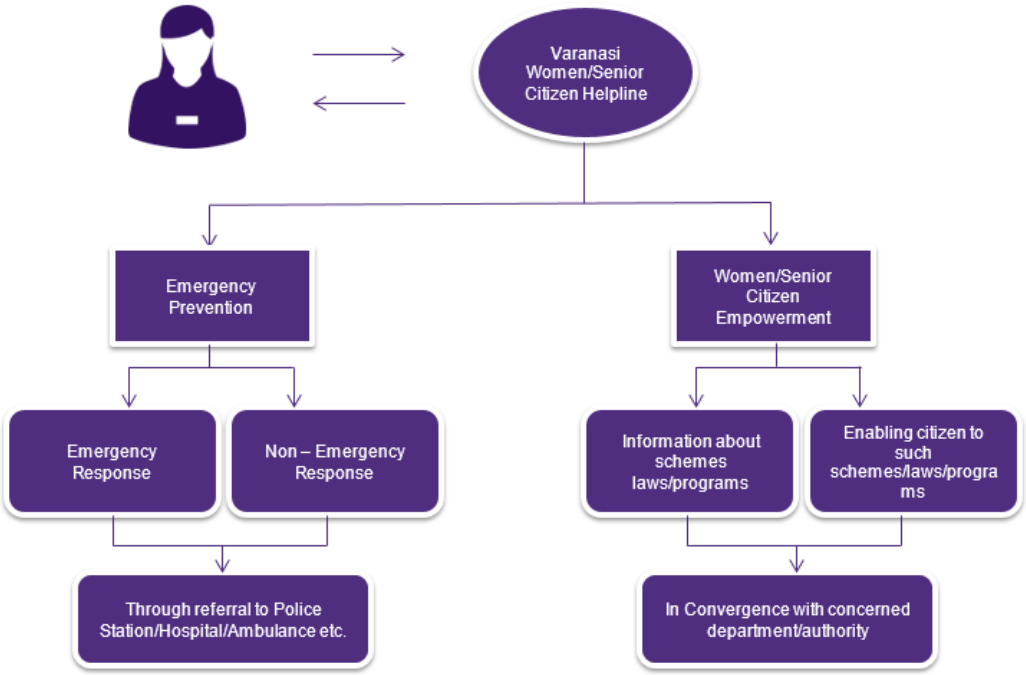
S.No.	Specifications
12	The application should allow service level plans to be varied by day, time of day, or a specific date.

Helpdesk/Contact Centre Executive/User/Operator System

S.No.	Specifications
1	It should provide consistent user interface across multiple media types like fax, SMS, telephone, email, and web call back.
2	The executive's desktop should have a "soft-phone" – an application that enables standard telephony functions through a GUI.
3	It should provide the executives with a help-desk functionality to guide them to answer a specific query intelligently.
4	It should also provide an easy access to executives to previous similar query which was answered successfully.
5	It should also be possible to identify a request to be a similar request made earlier.
6	It should be possible for executives to mark a query as complex/typical and put in to database for future reference by other agents.
7	It should be possible for executives to escalate the query.
8	System should be able to integrate with e–mail / sms gateway so that appropriate messages can be sent to the relevant stakeholders after the interaction and any updates thereon.
9	Should intelligently and automatically responds to email inquiries or routes inquires with skills based routing discipline to agents.

4.11 Women & Elderly Helpline

Diagrammatic View of the Women/Citizen Helpline



Accessing Helpline

The Helpline should be accessible 24 hours a day 7 days a week to any citizen suffering violence or in distress in the following manner:

- *Telephone* - landlines, mobile phones through calls, SMS/text messaging, mobile apps and fax messages;

- *Internet* - emails, web-posts, web-interface, social networking sites i.e. web page, facebook, twitter, mygov etc

- *Helpline* should be sensitive to the needs of persons who are hearing and speech impaired or people with disability. In case any citizen has been interrupted during his/her call or is unable to specify his/her problem or his/ her address due to being sick/disabled then the same would be traced and within minutes Helpline will facilitate an emergency response through nearest police station/ hospital or OS.

Service Description

Type of Service	Description
Violence Against Citizens Prevention	As soon as an Aggrieved Citizen (AG) or somebody on their behalf will contact WHL, her information would be attended by the call responder appointed there. Based on the urgency and the requirements explained by the caller, the responder will refer her to relevant support services like medical aid, police assistance or connect her to One Stop Center(OSC) for professional counselling, shelter, legal aid etc; if the woman needs to be rescued from a violent situation or is in urgent need of medical assistance then the PCR (Police Control Room) Van from the nearest police station or ambulance from nearest hospital service would be dispatched.
Information of Women/Senior Citizen Empowerment Schemes and programmes	WSCHL will provide information about the laws, existing schemes and government programs related to women empowerment and protection. Any woman in need of such information or someone on her behalf may call WSCHL which will provide this information or refer the woman to the relevant department to access the same. WSCHL will also provide guidance to women about processes to be adopted for accessing benefits of these schemes and programs.

Call Record Management (CRM) Application Software

The CRM application would have two modules –

a. Executive Module
b. MIS Reporting Module

CRM-Executive Module

The CRM-Executive Module should maintain complete call history record of all calls received in Helpline since the first day of its coming into being. The application should allow executives to capture and display caller information, problem descriptions, problem categorization, severity classification, prioritization, and complete status tracking with open and closed dates and times. Main features of the CRM-Executive Module application shall be as follows:

- It should support multiple host connectivity- local as well as remote
- It should have a single interface for consistent customer interactions through multiple touch points. It shall have a consolidated view of the caller to ensure that each executive has complete knowledge of every interaction regardless of the channel of communication.
- Each call record should be uniquely identifiable by an automatically generated query number. The unique query number will be intimated to the caller so that the same number is quoted by the caller during his/her subsequent call to know the status of any pending query/grievance
- The caller details, e.g., name, address, contact details (telephone no., fax no., mobile no., email-id), age, sex etc., will be recorded.
- Brief description of query/complaint of the caller should be recorded and details would be sent to citizen through SMS/E-mail.
- Category of each query should be recorded
- Brief description of answer/solution given by Executive should be recorded

- Call Center shall have the provision for call escalation to next level by Workflow with respect to the scheme/service defined by the User Department. The escalation would also reach the concerned officer by e-mail and SMS. There should also be provision for initiating automatic generation and sending of reminder Email for an escalated call for which reply is still awaited.

- Status of call should be recorded.

- The workflow for the next level should be provided as part of the CRM-Application Software

- Response from the next level Agency is recorded.

- Database of relevant next level agencies with their contact details (as provided by line department) to whom the caller can be referred for further details or to whom queries can be forwarded shall be maintained using the Back Office Database.

- Facility for searching the call record database on various attributes and combination of attributes would be provided.

- The application would also have the provision to build database of FAQs and their standard answers

- Database of all calls received since start of operations to be maintained

- Backup of the database would be maintained as per a well-defined backup policy

CRM-MIS Reporting Module

A web enabled Management Information System (MIS) would be developed to provide a user friendly and easily accessible one single portal giving due regard to the confidentiality of women affected by violence. When an aggrieved woman approaches the WSCHL her personal and case details will be fed into this system as per the prescribed format and a Unique ID Number would

be generated through which the case would be followed by the authorities from district to central level.

The CRM application should have a report generation module providing various MIS and statistical reports based on the call records database as required by VSCL from time to time. The user should be given the choice to set various filters like period (from-date and to-date), state, district, type of caller, escalation indicator, escalated to and various other attributes and their combinations while generating an MIS report from the database. A list of MIS Reports envisaged for the Helpline is given below. However, this is not an exhaustive list, and more no. of MIS Reports may be developed in line with the requirement of VSCL.

Also there should be logins created for respective Department HOD, and any discrepancies of higher priority get notified to them via SMS. They could also see the detailed statistics in accordance with their needs which would be customized.

Some ad-hoc MIS Reports may also need to be generated as and when required by Department. The ad-hoc reports may be required for various reasons including addressing a parliament question if any. Examples of such ad-hoc queries are:

- No. of complaints received against a particular service
- No. calls received from a particular Ward
- No. calls received for a specified service

The Command and Control Centre shall be able to respond in the Regional Language, Hindi, and English and agents should be able to effectively service stakeholders and beneficiaries from different parts of the City.

This system would also be used to access accurate information about the network of institutions and resources available and able to provide medical, legal, shelter support to citizens in the City. For the purpose, a Resource Directory would be collated from resource mapping at the City level and uploaded in the computer managed by the IT Staff.

Furthermore, this software should be utilized to provide information about all the schemes and programmes run by Central/State Government Administration for the empowerment of citizens. In case, a woman places a call to inquire about the same, she will be provided with

requisite information and guided through the process required for accessing these schemes and programmes. For example if a woman calls HL seeking information about widow pension scheme, the same would be provided to her along with the details of officer concerned (in particular ward where she resides) whom she needs to approach for accessing the same.

Reports

Every day the data of the last 24 hours would be extracted and analysed by Helpline Manager and a daily progress report (DPR) would be send directly to Authority, VSCL mentioning the challenges faced.

A monthly progress report (MPR) along with quarterly physical and financial reports (QPR) will be sent to the Head of the Dept.

CCC Technology

The identified Service Provider should deploy the latest technology in the proposed CCC solution for the Department.

Interactive Voice Response (IVR) Menu System

- Receive all inbound calls on the telephone number specified and prompts the callers to make their selection(s)

- Identify customer through CLI and support intelligent call routing (data from operators/ Government departments will not be provided). Firm will have to build its own data base of beneficiaries/residents over a period of time through calls received.

- Provide an easy to configure system that enables the users to change the IVR tree with no hard coding

- Support messages scheduling

- The IVR solution must be capable of capturing usage details of each caller as the caller goes through with the call. The IVR solution should have an interface through which usage details can be shared with other solutions.

- The IVR must integrate with the rest of the proposed solution to provide seamless call center performance

Automatic Call Distribution (ACD)

ACD system shall have the following functionalities:

- Perform call distribution and routing to the agent on "longest idle time" basis

- Queuing or holding the call for an agent if none is immediately available Provide the capability of combining data with the Interactive Voice Response (IVR) menu system that can intelligently route calls.

- Provide highly configurable system for adding/removing users, assigning users to different queues and defining skill sets

- Keep callers informed as to the status of the call and provide information to callers while they wait in queue

- Skill Based Routing and other intelligent routing methods

- Be designed such that it can handle high call volumes efficiently

- Support multiple groups for all call types

- Support the relaying of the information messages (marketing messages) to voice

- Have real time display features on digital phones

- Give unique identification of each Agent

- Trace malicious calls

- Contain monitoring and reporting tools for supervisor position

- Seamlessly integrate with the PBX.

- Have extensive reporting capabilities including but not limited to: Queue analysis reports such as total number of calls, total talk time, average call time, average speed of answer, abandoned call rate, average delay before abandon, average hold time Agent reports such as Login, Logout time, Idle time, average speed of answer, average handling time, number of Dropped Calls

Computer Telephone Integration (CTI)

- The CTI functionality shall support relevant screen pop-ups on the agent's screen on the basis of CLI (Caller Line Identity), ANI (Automatic number identification), DNIS (Dialed number identification sequence)

- The CTI shall be suitably integrated with the CRM and other applications used by the Command and Control Centre to send/receive data which needs to be populated on agent screen

- The CTI shall enable a computer application to take control of the call flow inside the Switch/EPABX & also allow the computer application to decide the most suitable action / agent for an incoming call

- On transferring the call to another agent the screen too should be transferred to that Agent's screen. Call events should be handled from the system such as hold, retrieve hold, conference, transfer etc.

- The CTI link shall pass events & information of agent status & changes in agent status as well as incoming calls to the computer applications

Dialer

A predicative dialer for outbound calls would be required; it should also be able to support specific programs if being run for the target segment.

Call Logger/ Recording

- The voice logger system shall provide recording of all inbound as well as outbound calls. 100% recording of calls and approximately 20% of agent screen action recording (for critical inputs) is to be provided. The recording should contain detailed call information and the solution must provide advanced search capabilities

- The recordings shall contain detailed call information including the entire recorded call, as well as the date, time, call duration, agent ID, called / caller number and unique identifier etc.

- Calls shall be stored for 30 days and shall be securely archived for at least one year thereafter. The archival media(tapes) will be provided by the firm. Wherever, dept mandates (subscription based services) storage for one year, Command and Control Centre would have to maintain the same.

Call Center Application

Call center application should have following features:

- Support Ticket with all related data logging and tracking and show all subsequent responses to a particular ticket number in thread view on same screen.

- Indexing and meta-tagging of all information like FAQ, schemes related data etc.

- Enable Managers / Supervisors to monitor the overall performance of the Call Center agents.

- Call center application must also interface with Other department /Stake holder department Application to retrieve information which would be required by the agent.

- Integrate with the CTI and should be able to pull IVR usage details of the caller including all options selected by the caller and all details entered by caller from the time the caller reaches an agent.

- Agent should be able to log and track each ticket. Information on the escalated tickets should also be made available as and when required by the agent.

Information, Complaint processing and satisfactory complaint disposal:

All Complaints on receipt should be informed by email and SMS immediately to the concerned officials or any other authority specified by the Department. All complaints will be processed by authorized persons of the Department in a time bound manner. It will be firm's responsibility to develop a proper monitoring mechanism in consultation with the Department to ensure that all the complaints are processed without undue delay.

Pending complaints should be regularly reviewed for immediate disposal by the competent authorities. If required, Bidder has to provide application login to all concerned disposal officers across Varanasi. The concerned authorities should be regularly reminded regarding pendency of their complaints and a regular list of such authorities where complaints are pending should be made available by the system as a part of the escalation process. All these reports would be used for analyzing the nature of complaints, severity levels and various other analytics to be carried by the Command and Control Centre to make this service more effective. For transparency & caller satisfaction, at different stages (ticket generation, complaint resolution) of compliant disposal, system should send an automated message at the caller number with details of ticket (number, expected time of resolution etc.) and its resolution, if any.

Customer relationship management application (CRM)

Command and Control Centre firm shall deploy its own Customer Relationship Management (CRM) software, customized as per Department requirement; to take care of all the services required to be undertaken by the agents. Some of its features are mentioned above.

The CTI/ CRM functionality shall support relevant screen pop-ups, on the agents desktop on the basis of CLI, DNIS (Dialed number identification sequence) etc. The agent application shall be GUI based. Agent shall capture details on the CRM for every call/application, (the list below is not exhaustive)

Inbound Call

- CRM will capture the caller's complete information like name, address, mobile number, additional number if any.

- CRM to have two options if only a query then the call would go to information cell, its CRM should have FAQ ready for the agent to respond to the concerned query. If a grievance, then the agent will have to go ahead and lodge the grievance with one of the established portals of the Government. An SMS with grievance number will go to the customer.

- CRM to capture information about all officers. After lodging a grievance outbound agent will escalate the complaint to concerned officer. Depending on the problem type, area and district that grievance belongs to, SMS will also go to concerned officer.

- CRM to maintain Escalation process. All the information to be fed in the CRM against the grievance.

- CRM will send the closing SMS to the caller who has lodged a grievance.

Outbound Calls

- Whom did they call?

- Process specific information (as specified by the Department) CRM should have the facility that it should capture the numbers of all concerned officer staff in the system and map them with the type of complaints, district and area they are responsible for.

- CRM will also have the facility to update and add the officer or staff mobile number.

CRM shall also support report generation on any of the details captured and show the report in threading view.

Process Delivery

Interfacing requirements will be assessed based on the product and service requirements of the Authority, VSCL. The Department expects the Service Provider to ensure an end to end process delivery by entering caller's details in the Call Center solution, generating a ticket number for each unique query which can be provided to the back end as a link to pursue the query and bring it to its conclusion. Concerned officer/Nodal officer can view the remarks on the call center application for every ticket number generated (all subsequent responses will be shown in a thread to a particular ticket number). At different stages of the process (ticket generation and resolution), system will send an automated message at the caller number with details of ticket (number, expected time of resolution etc.)

In order to achieve this, the Service Provider is expected to create a back-end process for each and every activity to be offered through the call center and link it to concerned person/sections involved in the backend processing. If there isn't any back-end process or system not available with the department, the bidder has to develop the workflow for the same. The department expects that queries generated by the front end are send as and when the issue is raised by the citizen and at each stage the status is reported to the citizen. In this way the knowledge pool with the Command and Control Centre will get updated and aggregated and used for servicing subsequent calls.

Standard Operating Procedures:

General Instructions

- The helpline staff shall at all times be extremely polite and give a patient hearing to the caller.

- The helpline staff should reassure the caller that help is on its way.

- The helpline staff shall not insist on the caller disclosing his/her identity, unless the caller so agrees and should assure the caller that the confidentiality of his/her identity and contact information shall be maintained.

- A confidential record including identity and contact details of the caller (if provided), along with aggrieved woman's personal and case details and name of the officer to whom information was passed on with date and time will be fed in to a system as per the prescribed format and a Unique ID Number would be generated.

- As soon as the complaint is registered a call/text message (SMS) would be sent to the SHO/ DM/ SP/ DYSP/CMO/PO/DO of the district/area as required.

- This command control center should offer services in the following four categories to any woman or girl facing violence within public or private sphere of life or to any citizen seeking information about any government or general programmes or schemes:

    a. Information services

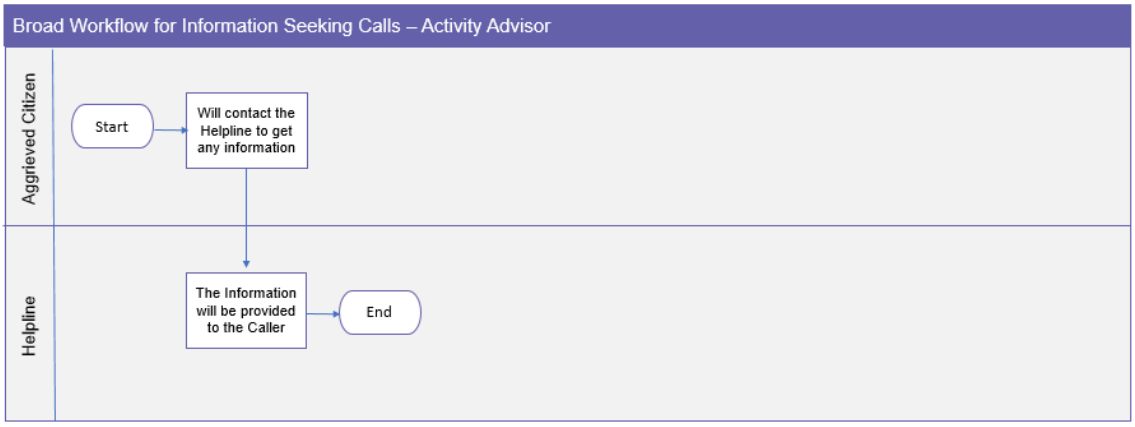
    b. Enquiry Services

    c. Request Services

    d. Grievances & Resolution

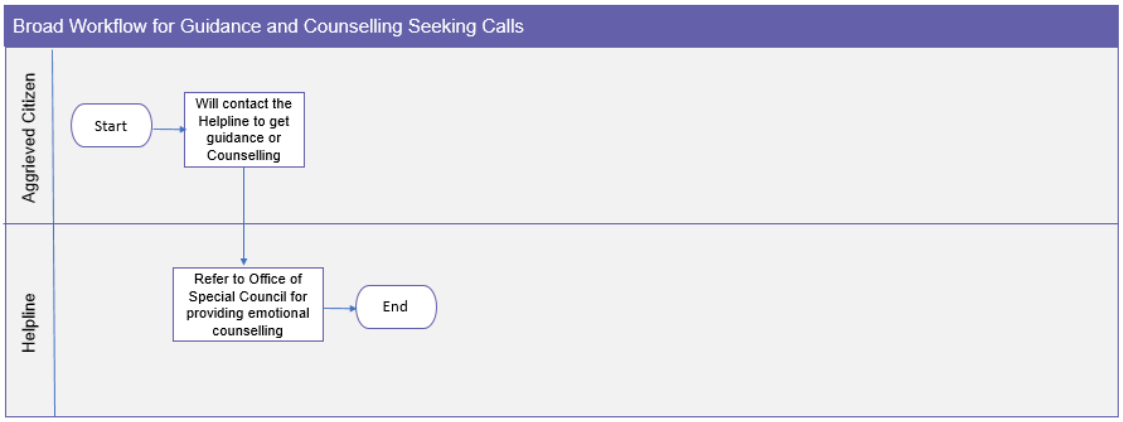
Information Services:

Any citizen can contact the Helpline Service to seek any of information about the different programmers and schemes available or any general information.



Enquiry Services

Any citizen can contact the Helpline Service to seek guidance and counseling in case of distress.



Case Specific Calls

- As soon as a call is received on the Helpline, the call responder shall listen to the caller patiently by keeping in mind physical/mental condition of the caller and shall take all possible information about the grievance of the caller (i.e. type of problem/grievance, his/her present location, type of help/assistance he/she

required etc.), including the details of the caller (whatever he/she discloses at that point of time without insisting too much on this aspect).

- The same shall be immediately passed to the local police, nearest PCR Van/Ambulance etc. as well as other concerned authorities/agencies as per the requirement.

- The call responder will also assure the caller of quick action and shall encourage the caller to keep patience and not to lose his/her control/temper/composure.

- After passing the information to all concerned authorities, a brief note about the caller, mentioning the maximum details available i.e. name, age, sex, present location, type of grievances/complaint, as well as the same of the officer to whom the call has been forwarded/entrusted for further action shall be fed into the software.

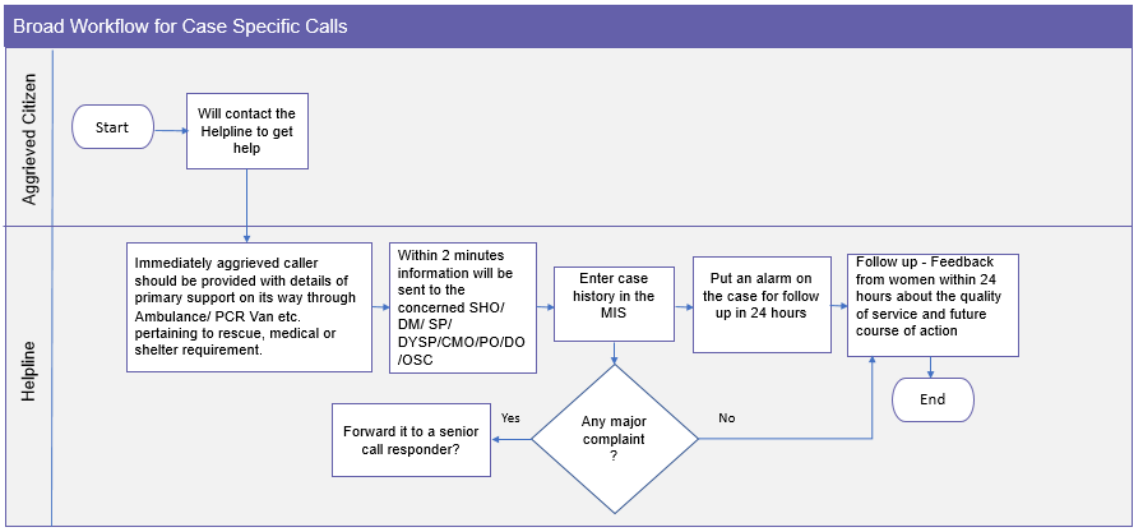
- Similarly, in case the information is received through text message, email or mobile app the concerned officials would be contacted to provide emergency support to the concerned citizen

- In case of requirement of police or medical assistance, the nearest PCR van or ambulance shall reach the caller at the earliest and shall provide all possible assistance to the caller without waiting for local police or hospitals and shall confirm their position at the spot.

- The PCR Van shall suo-moto respond immediately to any incident which unfolds before them or reported to them or brought to their notice. Under no circumstances shall the PCR van remain as mere spectator to the incident.

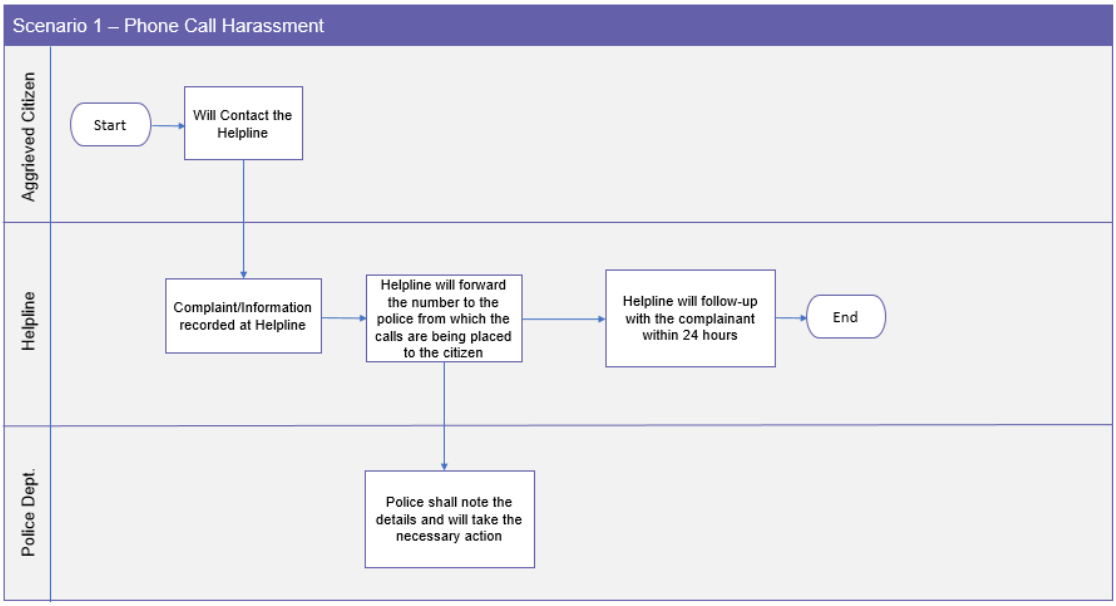
- The officer from the local police or other authorities to whom the information has been forwarded must reach the caller at the earliest without fail. Any delay on the part of the officer to whom the call has been marked will be viewed seriously.

- The concerned officer should reach the caller with all the required/necessary equipment i.e. first aid kit etc. Keeping the mental and physical condition of the caller in mind, maximum possible aid should be provided immediately.



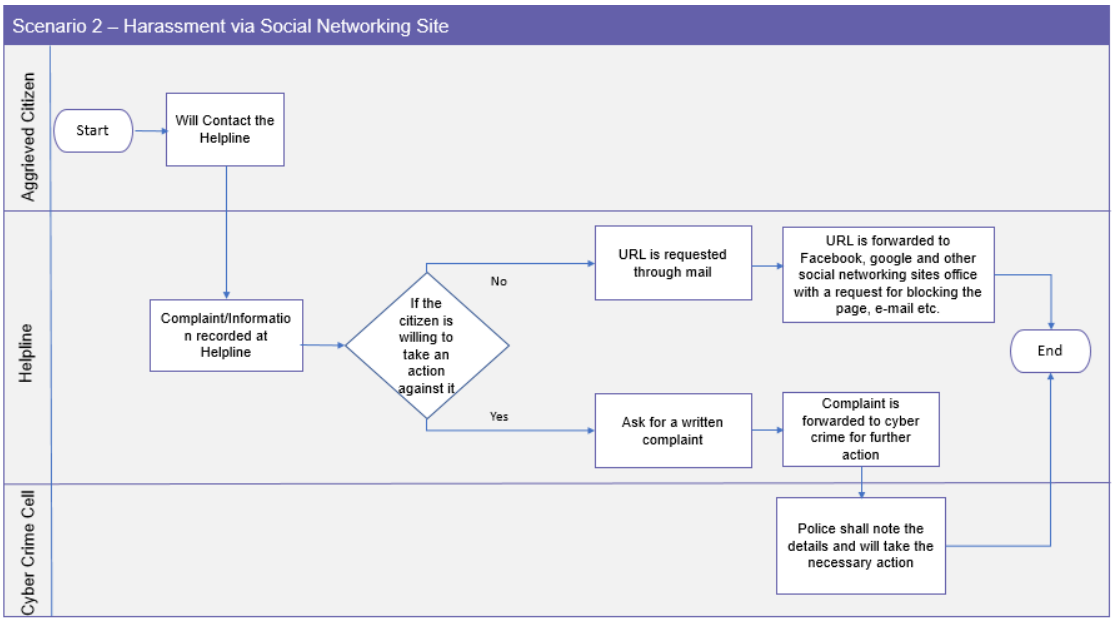
Scenario 1: Phone Call Harassment

1. The Aggrieved Citizen will contact the Helpline service.
2. The Executive shall note the number from which the harassment calls are being placed and forward it to the Police.
3. The Police shall note the details and take an action against the complaint made.
4. A follow – up call will be placed with the citizen within 24 hours to make sure that the issue has been resolved.



Scenario 2: Social Media Harassment

1. The Aggrieved Citizen will contact the Helpline service.
2. The Executive shall note the details of the case.
3. Will confirm if the citizen is willing to take an action.
4. If the citizen is willing to take an action against the offender
    - If Yes, then a written complaint is asked from the caller. After receiving the complaint, the same shall get forwarded to the cyber-crime branch for further action.
    - If No, then the URL is requested via mail which will be forwarded to the social networking site for getting it blocked.



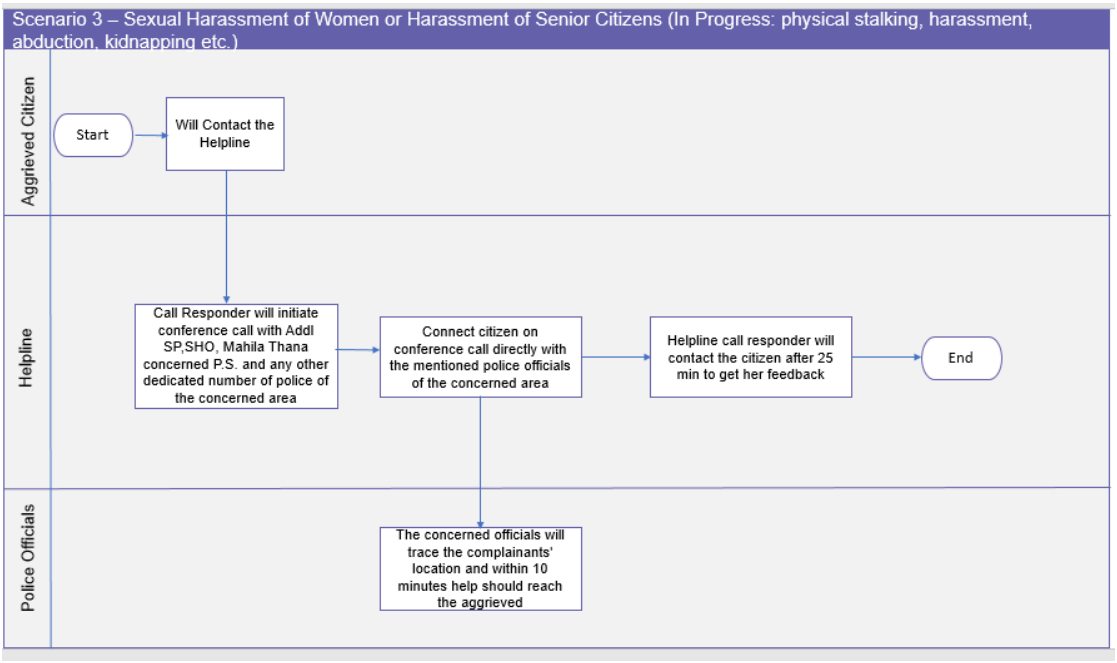
Scenario 3: Sexual Harassment of Women or any kind of Harassment of Senior Citizens

1. The Aggrieved Citizen will contact the Helpline service.

2. The Executive shall initiate the call between the caller and the police or any concerned official.

3. The Concerned officials will trace the complainant's location and will reach within a span 10 mins for help.

4. The Caller needs to be contacted after 25 mins to check on the individual and get the feedback for the help received.



Scenario 4: In Case if the police is not registering complaint of the citizen

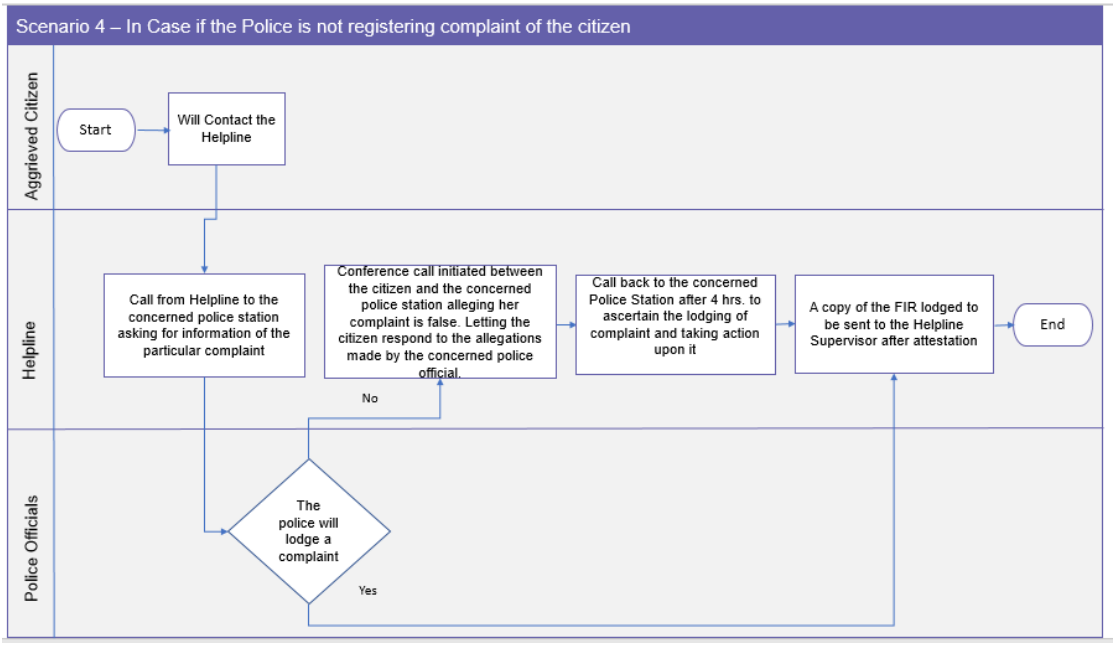
1. The Aggrieved Citizen will contact the Helpline service.

2. The Executive shall contact the Station to check the Status of the complaint lodged.

3. Lodging the Complaint

   - If Yes, then a copy of the FIR lodged will be shared with the Supervisor after Attestation.

   - If No, then a conference call will be initiated between the citizen and the concerned police station to resolve the issue. If the complaint is a false complaint, the case will be closed. A call will be placed to the police station after a period of 4 hours to check if the complaint was lodged and the copy will be shared with the Supervisor after attestation.



4.12 Network from Service Providers

Varanasi city has Reliance Jio, Powergrid, Vodafone, Airtel and BSNL as key players for laying of OFC across the city. All the vendors are available in all of ABD and PAN city areas. MSI has to analyse the quality of the connectivity across required locations for both the vendors and submit a detailed report along with bandwidth requirement across the city including DR. Based on the approval MSI has to execute the agreement with selected vendor for each location and add applications which can manage bandwidth and network availability and related SLA metrics, MSI should also consider a third party application to monitor and manage bandwidth. Procurement of network bandwidth services will be the responsibility of MSI and the cost should be borne by MSI during the entire contract period. As per TRAI guidelines, resale of bandwidth connectivity is not allowed. In such a case tri-partite agreement should be formed between Authority, selected MSI and Internet Service Provider(s).

Note: - The specifications provided in this RFP are indicative and carry guiding rule. The MSI may offer better products and solutions which meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards & best practices adopted in the industry. The MSI is encouraged to design an Optimized solution which is technically superior, innovative, proven, better in terms of functionality and is cost effective. Any specified parameters mentioned in the scope/technical

requirement in the RFP may be considered if it is required for meeting current & future requirements during the contract period. The MSI is fully responsible for the specified outcome to be achieved.

5. PROJECT IMPLEMENTATION TIMELINES, DELIVERABLES AND PAYMENT TERMS

It is intended to implement the project in a phased manner approach, distributed in four phases as mentioned below:

Note: The following table with mile stones is indicative. MSI can have a separate plan in the interest of completing the project in time. For details of deliverables please refer to Project Management section in this document.

Project Deliverables, Milestones and Timelines:

S. No.	Milestone	Deliverables	Timelines (in Months)
	Phase 1	**Project Initiation**	T + 1 month
1	**Planning**	1. Detailed Project Plan 2. Survey and Detailed Design of all the solutions components 3. Design Approvals 4. Required Civil Infrastructure Plan & Approval	**T+1 months**
	Phase 2	**Project Implementation Phase**	**T +10 months**

2	**Project Implementation**	1. Weekly and Monthly Progress Reports 2. Hardware Supply and Installation Stage 3. Pilot Deployment 4. Prototype Acceptance and Factory Acceptance Testing 5. Software Development 6. Final Deployment and Documentation 7. System Integration 8. Testing- Performance, Scalability, Systems Integration, Stress Testing, Security Testing, Systems Acceptance Test, etc. 9. Develop Training Materials	**T+9 months**
	Phase 3	**Operational Acceptance & Training (T1)**	**T +12 months**
3	**Training and Go-Live**	1. Training & Change Management 2. User Training 3. Mobilization of required staff 4. Operational System Acceptance 5. KICCC, DC, DR certifications 6. Go-Live	**T + 11 months**
	Phase 4	**Operations and Maintenance phase**	**T +60 months**
4	**O&M**	MSI has to follow the SLA's defined during the maintenance phase. MSI will be solely responsible for the deliverables. SLA Compliance Reports, Audits **Note:** The following table with mile stones is indicative. MSI can have a	**T + 60 months**

		separate plan in the interest of completing the project in time. For details of deliverables please refer to Project Management section in this document.	

Note:

- T is the date of signing of contract with MSI
- T1 is the date of Go Live of the last Phase

Payment Terms:

1. The request for payment shall be made to the Competent 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 fulfillment of all the obligations stipulated in the Contract.

2. Due payments shall be made promptly by the Competent Authority, generally within sixty (60) days after submission of an invoice or request for payment by MSI

3. The currency or currencies in which payments shall be made to the MSI under this Contract shall be Indian Rupees (INR) only.

4. All remittance charges shall be borne by the MSI.

5. In case of disputed items, the disputed amount shall be withheld and shall be paid only after settlement of the dispute.

6. Any penalties/ liquidated damages, as applicable, for delay and non-performance, as mentioned in this RFP document, shall be deducted from the due payments of the respective milestones.

7. Taxes, as applicable, shall be deducted / paid, as per the prevalent rules and regulations

Payment Schedule:

Payments to MSI shall be made by the Competent Authority, after the successful completion of the target milestones (including specified project deliverables):

S. No.	Scope of Work	Timelines	Payment
1	Phase I Project Planning	T + 1 Months	10% of contract value
2	Phase II Implementation	T + 10 Months	35% of contract value
3	Phase III Acceptance Testing & Go-live	T1 = T + 12 months	20% of contract value
4	Operations & Maintenance phase for a period of 60 months from the date of Go Live of the last solution	T1 + 60 Months	35% of Contract Value in equal quarterly installments

6. ANNEXURES

a. Annexure A- List of existing important junctions in Varanasi

Sr. No.	Junction Name	Junction Details
1	**Aashapur chowraha**	• Four legged uncontrolled junction • Absence of road markings & traffic signage • Presence of a rotary to regulate traffic flow.
2	**Aasiyana tiraha**	• Four legged uncontrolled junction • Absence of road markings & traffic signage.
3	**Airport Tiraha**	• Three legged uncontrolled junction
4	**Amara Khairi chowk**	• Six Legged Junction • Vehicle underpass located at the junction Junction sees high traffic flows during peak hours • Absence of road markings & signage.
5	**Ambedkar chowraha**	• Four legged uncontrolled junction • High density traffic observed at this junction • Rotary regulates the traffic • Signal is not functioning
6	**Andhra Pul chowraha**	• Four legged controlled by traffic police man • Flyover along the traffic flow • High density traffic observed at this junction
7	**Badau chungi**	• Three legged controlled by traffic police man • High density traffic observed at this junction • Road towards Rajghat is closed
8	**Bhikaripur Tiraha**	• Three legged controlled by traffic police man • Traffic flow is getting obstructed by Chowki at centre of road

Sr. No.	Junction Name	Junction Details
		• Absence of road markings & signage.
9	**Bhojubeer Tiraha**	• Four legged, unsignalized intersection
		• Presence of a rotary
		• High density traffic observed at this junction
10	**BHU chowraha**	• Four legged junction controlled by traffic police man.
		• High density traffic observed at this junction
		• Absence of road markings & traffic signage.
11	**Biseswarganj Mandi Tiraha**	• Three legged, uncontrolled intersection.
		• High density traffic observed at this junction
		• Absence of road markings & traffic signage.
12	**Chandpur chowraha**	• Four legged junction
13	**Chandra Chowraha**	• Four legged, uncontrolled intersection.
		• High density traffic observed at this junction
		• Absence of road markings & traffic signage.
14	**Chitaipur**	• Four legged, uncontrolled junction
		• Average density traffic observed at this junction.
		• Absence of road markings & traffic signage.
15	**Chowkaghat**	• Four legged junction controlled by traffic police man.
		• High density traffic observed at this junction
		• Absence of road markings & traffic signage.
16	**Chowkaghat Light Signal Chowraha**	• Four legged junction controlled by traffic police man.
		• High density traffic observed at this junction
		• Flyover along the traffic flow

Sr. No.	Junction Name	Junction Details
18	**Dharmashala Tiraha**	• Four legged junction controlled by traffic police man. • Signal is not functioning • Absence of road markings & traffic signage.
19	**Englishiya Line Tiraha**	• Four legged uncontrolled junction • Absence of road markings & traffic signage. • High density traffic observed at this junction.
20	**Garwa Ghat Tiraha**	• Three legged, uncontrolled junction • Average density traffic observed at this junction. • Absence of road markings & traffic signage.
21	**Gilat Bazaar Chowki**	• Four legged uncontrolled junction • High density traffic observed at this • junction. • Absence of road markings & traffic signage.
22	**Girja Ghar chowraha**	• Five legged uncontrolled junction • Absence of road markings & traffic signage • High density traffic observed at this junction • Signal is not Functioning
23	**Godowliya chowraha**	• Four legged uncontrolled junction • High density traffic observed at this junction. • Presence of a rotary.
24	**Golgadda Tiraha**	• Three legged uncontrolled junction • High density traffic observed at this junction. • Absence of road markings & traffic signage
25	**Gurbagh Tiraha**	• Three legged uncontrolled junction • Absence of road markings & traffic signage.

Sr. No.	Junction Name	Junction Details
26	**Kajakpura railway crossing**	• Four legged junction controlled by traffic police man. • High density traffic observed at this • junction. • Presence of a rotary • Railway Line is crossing across the road
27	**Lahartara chowraha**	• Four legged, uncontrolled junction. • Absence of road markings & traffic signage. • Medium density traffic observed at this junction.
28	**Lahooravir chowraha**	• Four legged, uncontrolled junction. • Absence of road markings & traffic signage. • Signal is not functioning
29	**Lalpur Entry point**	• Four legged junction.
30	**Lanka Tiraha**	• Four legged, uncontrolled junction. • Absence of road markings & traffic signage. • High density traffic observed at this junction
31	**Lohta**	• Four legged junction.
32	**Mahmoorganj police chowki**	• Three legged, uncontrolled junction. • Absence of road markings & traffic signage. • High density traffic observed at this • junction. • Fly Over is under construction.
33	**Maidagyn Chowraha**	• Four legged, uncontrolled junction. • Absence of road markings & traffic signage. • Presence of a rotary.
34	**Maldahiya chowraha**	• Four legged, uncontrolled junction. • Absence of road markings & traffic signage. • Presence of a rotary.

Sr. No.	Junction Name	Junction Details
35	**Maruidih chowraha**	• Four Legged uncontrolled Junction • Absence of road markings & traffic signage. • High density traffic observed at this • junction.
36	**Mint house Tiraha**	• Three Legged Junction controlled by policemen • Presence of a rotary • Signal is not functioning
38	**Nadeswar Masjid Chowkagat**	• Three legged, uncontrolled junction. • Absence of road markings & traffic signage
39	**Nirmamai Tiraha**	• Four legged, uncontrolled junction. • Absence of road markings & traffic signage. • Rathayatra Kamacha Road is closed due to Construction.
40	**Pahariya Chowraha**	• Four Legged- uncontrolled Junction • Absence of road markings & traffic signage
41	**Pandeypur chowraha**	• Four legged junction controlled by traffic police man. • Absence of road markings & traffic signage. • Presence of a rotary
42	**Parao**	• Four legged junction
43	**Police Line Chowraha**	• Four legged junction controlled by traffic police man. • Presence of a rotary • Absence of road markings & traffic signage.
45	**Ramna chowki**	• Four legged uncontrolled junction • High density traffic observed at this • junction.
46	**Rath Yatra chowraha**	• Four legged junction controlled by traffic policeman • High density traffic observed at this

Sr. No.	Junction Name	Junction Details
		• junction.
		• Absence of road markings & traffic signage.
47	**Roadways Tiraha**	• Three legged uncontrolled junction
		• High density traffic observed at this junction
		• Absence of road markings & traffic signage
48	**Sajan Tiraha**	• Four legged uncontrolled junction
		• High density traffic observed at this junction
		• Presence of a rotary
49	**Tarikhana Tiraha**	• Three legged junction controlled by traffic police man.
		• Absence of road markings & traffic signage.
		• High density traffic observed at this junction.
50	**Tarna Overbridge**	• Four legged junction
51	**Teliyabagh chowraha**	• Four legged uncontrolled junction
		• Absence of road markings & traffic
		• Presence of a rotary.
52	**Tengra More**	• Four Armed Junction
		• Vehicle underpass located at the junction
53	**Bangalitola inter college chowraha**	• Four legged junction controlled by traffic police man.
		• Absence of road markings & traffic signage.
		• High density traffic observed at this junction
54	**Beniabagh Tiraha**	• Three legged uncontrolled junction
		• Presence of a rotary
		• High density traffic observed at this junction
55	**Kaal Bhairav Chowraha**	• Four legged uncontrolled junction
		• Absence of road markings & traffic signage.

Sr. No.	Junction Name	Junction Details
		• Presence of a rotary
56	**Kabir chowraha**	• Four legged uncontrolled junction
		• High density traffic observed at this junction
		• Presence of a rotary
57	**Kali Mata Mandir Chowraha**	• Three legged uncontrolled junction
		• High density traffic observed at this junction
		• Road is under Construction near the flyover
58	**Lohamandi chowraha**	• Four legged uncontrolled junction
		• Medium density traffic observed at this junction
59	**Luxa Thana**	• Three legged uncontrolled junction
		• High density traffic observed at this junction
		• Three legged uncontrolled junction
60	**Machodari**	• High density traffic observed at this junction
		• Absence of road markings & traffic signage.
		• Four legged uncontrolled junction
61	**Padmashree chowraha**	• Absence of road markings & traffic signage.
		• High density traffic observed at this junction
62	**Rewari Talabh Tiraha**	• Four legged uncontrolled junction
63	**Sarnath Tiraha**	• Three legged uncontrolled junction
		• Central Island is present in the road
64	**Sigra chowraha**	• Four legged uncontrolled junction
		• Presence of a rotary
		• Signal is not functioning

b. List of Identified Locations (Junctions) along with projected equipment

List of Junctions in Varanasi		No of Arms	No. of RLVD Camera	No. of ANPR Camera	No. of Fixed Box Camera	No. of Multi Sensor Camera	No. of Public Address System	No. of VMS
Sr. No.	Junction Name							
1	**Aashapur chowraha**	4	4	4	4	1	1	0
2	**Aasiyana tiraha**	4	0	0	4	0	1	0
3	**Airport Tiraha**	4	0	0	4	0	0	0
4	**Amara Khairi chowk**	6	6	6	6	1	1	0
5	**Ambedkar chowraha**	4	0	0	4	0	1	0
6	**Andhra Pul chowraha**	4	4	4	4	1	1	1
7	**Badau chungi**	3	0	0	3	0	0	0
8	**Bhikaripur Tiraha**	3	0	0	3	0	1	1
9	**Bhojubeer Tiraha**	4	0	0	4	0	1	1
10	**BHU chowraha**	4	4	4	4	1	1	0
11	**Biseswarganj Mandi Tiraha**	3	0	0	3	0	1	0
12	**Chandpur chowraha**	4	0	0	4	0	1	1
13	**Chandra Chowraha**	4	4	4	4	1	1	0
14	**Chitaipur**	4	0	0	4	0	1	0
15	**Chowkaghat**	4	4	4	4	1	1	1
16	**Chowkaghat Light Signal Chowraha**	4	4	4	4	1	1	0

List of Junctions in Varanasi		No of Arms	No. of RLVD Camera	No. of ANPR Camera	No. of Fixed Box Camera	No. of Multi Sensor Camera	No. of Public Address System	No. of VMS
Sr. No.	Junction Name							
17	**Dharmashala Tiraha**	4	0	0	4	0	1	0
18	**Englishiya Line Tiraha**	4	4	4	4	1	1	0
19	**Garwa Ghat Tiraha**	3	0	0	3	0	1	0
20	**Gilat Bazaar Chowki**	4	0	0	4	0	1	0
21	**Girja Ghar chowraha**	5	5	5	5	1	1	0
22	**Godowliya chowraha**	4	4	4	4	1	1	0
23	**Golgadda Tiraha**	3	0	0	3	0	1	0
24	**Gurbagh Tiraha**	3	0	0	3	0	1	1
25	**Kajakpura railway crossing**	4	0	0	4	0	1	0
26	**Lahartara chowraha**	4	4	4	4	1	1	1
27	**Lahooravir chowraha**	4	0	0	4	0	1	0
28	**Lalpur Entry point**	4	4	4	4	1	1	0
29	**Lanka Tiraha**	4	0	0	4	0	1	1
30	**Lohta**	4	4	4	4	1	0	1
31	**Mahmoorganj police chowki**	3	0	0	3	0	1	0
32	**Maidagyn Chowraha**	4	4	4	4	1	1	0

List of Junctions in Varanasi		No of Arms	No. of RLVD Camera	No. of ANPR Camera	No. of Fixed Box Camera	No. of Multi Sensor Camera	No. of Public Address System	No. of VMS
Sr. No.	Junction Name							
33	**Maldahiya chowraha**	4	4	4	4	1	1	1
34	**Maruidih chowraha**	4	0	0	4	0	1	0
35	**Mint house Tiraha**	3	0	0	3	0	1	0
36	**Nadeswar Masjid Chowkagat**	3	0	0	3	0	1	0
37	**Nirmamai Tiraha**	4	0	0	4	0	1	0
38	**Pahariya Chowraha**	4	0	0	4	0	1	0
39	**Pandeypur chowraha**	4	4	4	4	1	1	0
40	**Parao**	4	0	0	4	0	1	1
41	**Police Line Chowraha**	4	4	4	4	1	1	0
42	**Ramna chowki**	4	0	0	4	0	1	0
43	**Rath Yatra chowraha**	4	4	4	4	1	1	1
44	**Roadways Tiraha**	3	0	0	3	0	1	0
45	**Sajan Tiraha**	4	4	4	4	1	1	1
46	**Tarikhana Tiraha**	3	0	0	3	0	1	0
47	**Tarna Overbridge**	4	0	0	4	0	1	0
48	**Teliyabagh chowraha**	4	0	0	4	0	1	0
49	**Tengra More**	4	4	4	4	1	1	0

List of Junctions in Varanasi		No of Arms	No. of RLVD Camera	No. of ANPR Camera	No. of Fixed Box Camera	No. of Multi Sensor Camera	No. of Public Address System	No. of VMS
Sr. No.	Junction Name							
50	**Bangalitola inter college chowraha**	4	0	0	4	0	1	0
51	**Beniabagh Tiraha**	3	0	0	3	0	1	0
52	**Kaal Bhairav Chowraha**	4	0	0	4	0	1	0
53	**Kabir chowraha**	4	0	0	4	0	0	0
54	**Kali Mata Mandir Chowraha**	3	0	0	3	0	1	0
55	**Lohamandi chowraha**	4	0	0	4	0	1	0
56	**Luxa Thana**	3	0	0	3	0	0	0
57	**Machodari**	4	0	0	4	0	0	0
58	**Padmashree chowraha**	4	0	0	4	0	1	0
59	**Rewari Talabh Tiraha**	4	0	0	4	0	1	0
60	**Sarnath Tiraha**	3	0	0	3	0	1	0
61	**Sigra chowraha**	4	4	4	4	1	1	0
Total			**87**	**87**	**232**	**21**	**55**	**13**

c. Annexure C- Solid Waste Management System- existing infrastructure details:

Machines/ Vehicles for SWM under use			
Sr. No.	**Machines/ Vehicles**	**Number**	**Type**
1	Auto Rickshaw/hopper tipper	150	GPS
2	Compactor	30	GPS
3	Portable compactor	16	GPS
4	JCB	4	GPS
5	Tractor	3	GPS
6	Road sweeping machine	2	GPS
7	Bins	3000	RFID
8	No. of households (lakh)	20000	RFID

Material/ equipment under use		
Sr. No.	**Material/ equipment Used**	**Number**
1	**Road side bins(1.1 cum capacity)**	950
2	**D.P. container (3 cum capacity)**	10
3	**Wheel Barrow (110 ltr.)**	400
4	**Solo dustbin (150 ltr) with stand**	1000
5	**Handcart with 4 bins**	40
6	**Cycle rickshaw with 4 part plastic container**	50
7	**Dustbin (100 ltr.) with stand**	500
8	**Dustbins (4.5 cum capacity)**	158

Supervisory Staff		
Sr. No.	**Supervisors**	**Number**
1	**Supervisors**	90
2	**Sanitary Inspectors**	13

Solid Waste Management Site		
Sr. No.	**Vehicle types**	**Number**
1	Solid Waste Management Site/treatment plant	1

Intermediate dump yards (Kuda Ghar)	
Sr. No.	**Kuda Ghar**
1	I. D. H
2	Azad Park
3	Harteesth
4	Bakrabad
5	Senpura
6	Andhra pool
7	Near Nagam Diesel Pump
8	Pitaskunda
9	Gadolia
10	Prachi
11	Benia
12	Hadda Sarai
13	Lahartara pool
14	Circuit house
15	Ardali Bazar
16	Tehsil
17	Shivpur
18	Deendayal Road
19	Kashiram Yojana (3rd Day)
20	Rangoli chawrah Sarnath (3rd day)
21	Kait (2nd day)

d. Annexure D- Details of lights available in the Area Based Development (ABD) Region of Varanasi

List of wards in ABD area of Smart City				Available Lights						
S No.	**Ward No.**	**Ward Name**	**Ward Coverage**	**20 W**	**40 W**	**70 W**	**120 W**	**160 W**	**200 W**	**Total**
1	8	**NAGWA**	Part	5	13	83	12	0	20	133
2	17	**SHIVPURWA**	Part^	115	124	250	13	0	0	502
3	31	**LOCO CHHITTUPUR**	Part^	234	4	236	25	0	40	539

4	32	**NARIYA**	Part	0	63	153	13	0	0	229
5	35	**KAJIPURA**	Part*	0	0	196	0	0	0	196
6	39	**SHIVALA**	Full	0	0	0	0	0	0	0
7	40	**SIGRA**	Part	2	77	278	9	0	19	385
8	44	**BHELUPUR**	Part	1	6	95	22	0	0	124
9	45	**CHETGANJ**	Part	0	143	182	18	0	0	343
10	49	**JANGAMBARI**	Part	o	0	5	3	0	0	8
11	51	**DARANAGAR**	Part	0	0	191	0	0	0	191
12	52	**PIYARIKALA**	Part^	7	140	91	4	0	0	242
13	54	**BHADAINI**	Part	4	1	8	3	0	0	16
14	59	**LAHANGPURA**	Part	0	51	170	0	0	0	221
15	60	**LUXA**	Part	0	214	147	8	0	1	370
16	61	**PANDARIBA**	Full	0	3	235	5	0	0	243
17	62	**RAJ MANDIR**	Part	0	1	8	3	0	0	12
18	63	**GARHWASI TOLA**	Full	0	21	29	3	0	25	78
19	64	**RAMAPURA**	Full	0	0	0	0	0	0	0
20	65	**BAGHARA**	Full	0	0	0	2	0	0	2
21	67	**GOLA DINANATH**	Part	0	0	0	0	0	0	0
22	68	**BENIA**	Full	0	1	0	1	0	0	2
23	69	**SARAI GOWARDHAN**	Part	0	0	0	0	0	0	0
24	70	**PANDEY HAWELI**	Part*	5	9	7	0	0	0	21
25	72	**REWARI TALAB**	Part	0		179	0	0	0	179
26	73	**LALLAPURA KALA**	Part	0	99	57	0	0	0	156
27	74	**DASHASHWAMEDH**	Full	0	0	0	0	0	0	0
28	78	**BENGALI TOLA**	Full	0	1	0	0	0	0	1
29	79	**HARHA SARAI**	Full	0	4	7	1		0	12
30	83	**KALBHAIRAV**	Part	3	7	17	20	12	0	59
31	90	**MADANPURA**	Part	0	0	0	0	0	0	0

*Maximum area of ward covered

^Littile area of ward Covered

Note:

- The total lights to be converted into smart lights also covers the lights existing in the nearby/ adjacent wards to the ABD area.

- Total no. of lights' conversions to be done for 10,000 lights. The list of all wards is enclosed on Annexure 'D'.

e. Annexure D- Lists of Wards

Ward Number	Ward Name		Ward Number	Ward Name
1	INDRAPUR		**46**	KAMALGARHA
2	VINAYAKA		**47**	OMKALESHWAR
3	TARNA		**48**	MADHYAMESHWAR
4	RAJGHAT		**49**	JANGAMWARI
5	NARAYANPUR		**50**	SARAIYA
6	SIRSAULI		**51**	DARAGANJ
7	HUKULGANJ		**52**	PIYARIKALA
8	NAGWA		**53**	BIRDOPUR
9	LAHARTARA		**54**	BHADAINI
10	SUNDERPUR		**55**	ISHWARGANGI
11	CHAWKAGHAT		**56**	JALALIPURA
12	TULSIPUR		**57**	DIDHORI MAHAL
13	SARAI SURJAN		**58**	NAWAPURA
14	NAWABGANJ		**59**	LAHANGPURA
15	NADESAR		**60**	LUXA
16	DINDAYALPUR		**61**	PANDARIBAGH
17	SHIVPURWA		**62**	RAJ MANDIR
18	KHAJURI		**63**	GARHWASI TOLA
19	SHIVPUR		**64**	RAMAPURA

20	SIKRAUL		**65**	BAGHARA
21	HABIBPURA		**66**	PRAHLAD GHAT
22	RAJABAZAAR		**67**	GOLA DINANATH
23	ALAIPURA		**68**	BENIA
24	JAGATGANJ		**69**	SARAI GOWARDHAN
25	JOLHA		**70**	PANDEY HAWELI
26	RAMREPUR		**71**	PATHANI TOLA
27	MAWAIYA		**72**	REWARI TALAB
28	NEWADA		**73**	LALTAPURA KALA
29	NAI BASTI		**74**	DASHASHW AMEDH
30	SARNATH		**75**	DHUP CHANDI
31	LOKO-CHITOPUR		**76**	RAHIPURA
32	NARIA		**77**	BALUABIR
33	PANDEYPUR		**78**	BENGALI TOLA
34	KONIA GAO		**79**	HARHA SARAI
35	KAJIPURA		**80**	KATEHAR
36	PAHARIA		**81**	JAMALUDDINPUR
37	LALAPUR KHURD		**82**	BANDHU KACCHIBAGH
38	BAJADIHA		**83**	KAL BHAIRAV
39	SHIVALA		**84**	KAMLAPURA
40	SIGRA		**85**	BASNIA
41	KAMESHWAR MAHADEV		**86**	KHOWAJA SADDULAPURA
42	KATUPURA		**87**	AAGAGANJ
43	KHOJWA		**88**	RASULPURA
44	BHLUPUR		**89**	CHHITANPURA
45	CHETGANJ		**90**	MADANPURA

f. Annexure E- Environment Monitoring System

Environment/ Pollution Monitoring System		
1	**No. of Pollution Inspection Centre**	12
2	**Equipment**	1. Interceptor (breath enhalater, Speed check) 2. Publicity Van 3. Pollution check Vehicle
3	**Plan for Pollution exemption idea**	e-Rickshaw, Permit (CNG & LPG)

g. Annexure D- Highways passing through Varanasi City

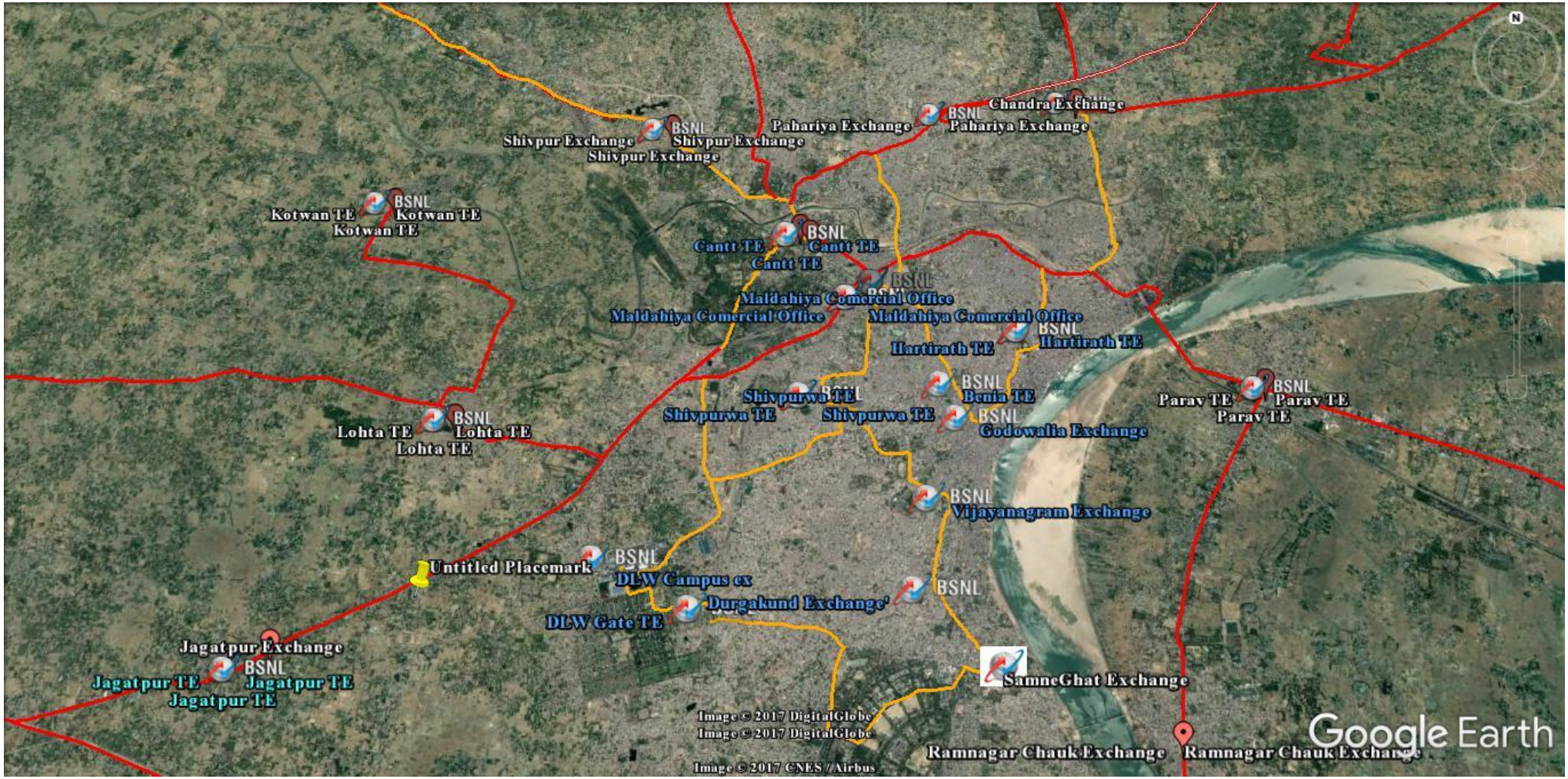
S.No.	National Highways	Route	State Highways
1	**NH-2**	GT road from Mughal Sarai to Allahabad	SH-87
2	**NH-7**	Hyderabad gate in Varanasi to Jabalpur, Hyderabad, Madurai, etc	SH-73
3	**NH-29**	Varanasi to Gorakhpur, Kushinagar.	SH-74
4	**NH-56**	Varanasi to Jaunpur Lucknow.	SH-98

h. Annexure E- List of existing Wi- Fi Hot spots across Varanasi city by BSNL as Network Service Provider

Sl. No.	Site Name
1	KABIRCHAURA HOSPITAL
2	DEEN DAYAL HOSPITAL
3	APEX HOSPITAL
4	VIKASH PRADHIKARAN
5	GODOWLIA CHAURAHA
6	ITI KARAUNDI
7	BIG BAZAR
8	MALDAHIA CSC
9	PCF PLAZA
10	HARAHUA BLOCK
11	CHOLAPUR BLOCK
12	KASHI VIDYAPEETH
13	PINDARA BLOCK
14	CHIRAIGAON BLOCK
15	DEEDH BLOCK
16	SBI ZONAL OFFICE
17	GYANPUR
18	DURGAKUND EXCHANGE

19	GYANVAPI TIRAHA
20	BHU GATE
21	SHASHTRI NAGAR MARKET
22	RAVINDRA NATH TAGORE
23	KUBER COMPLEX
24	ANANDMAYI HOSPITAL
25	RATHYATRA CHAURAHA
26	UP COLLEGE
27	GALAXY HOSPITAL
28	GOLGHAR KUTCHERY
29	HOTEL MADIN
30	HOTEL D'MERIDIAN
31	VINAYAK CHAURAHA
32	SUNBEAM SCHOOL MGS
33	HINDU INTERNATIONAL SCHOOL

i. Annexure G- Network Map of OFC by BSNL as Network Provider



j. Annexure H- Network Map of OFC by Reliance Jio as Network Provider