Request for Proposal

for

Selection of System Integrator for Operation, Maintenance & Technical Support for Jana Sunani Portal

RFP No.: OCAC-SEGP-SPD-0083-2025-26021

Vol-II (Terms of Reference)

ODISHA COMPUTER APPLICATION CENTRE

[TECHNICAL DIRECTORATE OF E&IT DEPARTMENT, GOVERNMENT OF ODISHA]

OCAC Building, Acharya Vihar Square, Bhubaneswar-751013, Odisha, India
W: www.ocac.in | T: 0674-2567295/2567283 | F: 0674-2567842

Table of Contents

1 About Department

The Electronics & Information Technology Department, Government of Odisha, is the nodal department responsible for the formulation, implementation, and promotion of policies related to e-Governance and Information Technology in the state. The department plays a pivotal role in leveraging ICT (Information and Communication Technology) to enhance public service delivery, ensure transparency, and improve citizen engagement across government systems.

As a key driver of Odisha's digital transformation initiatives, the department oversees the development and maintenance of critical digital infrastructure and citizen-facing platforms. One such flagship initiative is the Jana Sunani Portal—Odisha's unified public grievance redressal mechanism—enabling citizens to lodge complaints and monitor their resolution through a centralized, transparent, and tech-enabled interface.

1.1 Jana Sunani Portal

The Jana Sunani Portal is the Unified Public Grievance Redressal System of the Government of Odisha, to ensure transparent, accountable, and responsive governance. It serves as a one-stop platform for citizens to register grievances, track their status, and receive timely resolutions from concerned government departments and authorities.

The portal integrates grievance redressal mechanisms across departments, districts, and blocks, creating a seamless digital ecosystem where public complaints are acknowledged, assigned, processed, and resolved in a time-bound and efficient manner.

Key Features:

- **Multi-Channel Accessibility:** Citizens can lodge grievances through the web portal, mobile app (Android/iOS), WhatsApp, call centers, email, and letter submissions.
- **Unique Ticketing System:** Each grievance receives a unique Ticket ID for transparent tracking.
- **Real-Time Status Updates:** Citizens are notified of updates at every stage via SMS and email.
- **Role-Based Workflow:** The portal features a hierarchical escalation matrix, ensuring accountability at every administrative level.

- **Dashboard & Analytics:** Government officials have access to comprehensive dashboards and MIS reports for real-time monitoring and performance evaluation.
- **Language Support:** Available in both English and Odia for ease of access to all users.
- **Time-Bound Redressal:** Grievances are to be addressed within a defined time frame.

User and Stakeholder Details:

State Level Authorities	❖ Office of Hon'ble Governor. ❖ Office of Hon'ble Chief Minister. ❖ Chief Secretary ❖ Development Commissioner ❖ DG & IG Police. ❖ Department Head (Secretaries) ❖ Revenue Divisional Commissioner. ❖ Heads of Autonomous bodies & agencies. ❖ Directors
District Level Authorities	❖ Collectors ❖ Superintendent of Police. ❖ Project Director, DRDA ❖ Chief District Medical Officer ❖ Chief District Veterinary Officer ❖ Chief District Agriculture Officer ❖ District Social Welfare Officer ❖ Civil Supply Officer ❖ District Education Officer
Block/Tehsil/ Municipal Level Authorities	❖ Block Development Officer. ❖ Tehsildars Executive Officers of Urban Local Bodies (ULBs)

2 Background

2.1 Existing Jana Sunani Portal

While the Jana Sunani Portal has significantly improved public grievance redressal mechanisms in Odisha, certain operational and technical challenges have been identified over time that hinder its full potential. These challenges necessitate system enhancements to further improve user experience, efficiency, and accountability.

- User Experience & Accessibility Issues
- Grievance Tracking & Transparency Gaps
- Escalation & Accountability Bottlenecks
- System Performance and Scalability
- Data Analytics and Decision Support
- Feedback Mechanism

2.2 Existing Modules/Sub Modules

Sl#	Module Name	Functionalities
a)	Grievance Registration	Citizens can lodge complaints through various channels, including the Website, WhatsApp, Email, Postal Letters, Social Media, Direct Submissions, and Mobile Application. This flexibility ensures accessibility for all users
b)	CM Grievance Appointment Booking System	This module allows citizens to book appointments to meet the Chief Minister to represent the grievances.
c)	District-Level Joint Hearings	Citizens can access information about joint hearings conducted by District Collectors and Superintendents of Police, providing an opportunity to present their grievances.
d)	Grievance Status Tracking	After registering a complaint, users can monitor its progress online, providing transparency and keeping citizens informed about the resolution process.

e)	Admin Login	Designated government officials have access to an administrative interface for managing and addressing grievances. This module ensures that complaints are directed to the appropriate departments for timely resolution.
f)	Mobile Application	The Jana Sunani mobile app extends the portal's functionalities to smartphones, allowing users to register grievances, track their status, and access other services on the go.
g)	Contact Information	Users can find contact details for further assistance, ensuring they can reach out for support when needed.
h)	Frequently Asked Questions (FAQs)	This section provides answers to common queries, assisting users in understanding the portal's features and the grievance redressal process

2.3 Existing Technology

The following technologies are used in the existing Jana Sunani Portal.

Sl#	Category	Software Title
a)	Operating System	Linux
b)	Platform/ Language	PHP, Android, iOS
c)	Database	MySQL
d)	Web Server	Apache
e)	IDE	Visual Studio code
f)	Service	Rest API
g)	Depending Module	Laravel, Python

3 Objective

OCAC on behalf of General Administration and Public Grievance Department, Govt. of Odisha intends to engage qualified System Integrator to carry out the project which includes:

- Takeover of existing Jana Sunani Portal
- Technology Enhancement
- Enhancement and Modernization of Present Application
- Post implementation support (onsite & offsite)

4 Scope of Work

4.1 Migration & Takeover of Existing Jana Sunani Portal

The primary objective is to ensure uninterrupted continuity of the Jana Sunani application from the date of Work Order issuance. The System Integrator (SI) shall ensure the seamless transition of the application, infrastructure, and services within 15 days from the issuance of the work order, ensuring optimal performance and timely issue resolution as per the transition plan. Prior to the end of the Transition Phase, the SI must demonstrate a clear understanding of the application and readiness for independent operations.

During the Knowledge Transfer and Data Migration Phase, the SI shall:

a) Review technical documents and source code provided by the department.
b) Conduct detailed knowledge transfer sessions with the current service provider.
c) Define all the specifications required to populate data into the proposed system.
d) Prepare a comprehensive data cleaning and migration plan and submit it to the concerned authority for approval.
e) Undertake uniform codification and classification of all data sets in alignment with the new system's data architecture.
f) Identify, configure, or develop appropriate tools/programs for secure data upload and download during migration.
g) Ensure minimum business downtime during the data cleaning and migration process.
h) Verify the accuracy, integrity, and completeness of the migrated data to avoid data loss or discrepancies.
i) Complete the migration of all required data prior to the go-live of the new system.

j) Migrate the database from the existing system to the newly developed platform, including structured, semi-structured, and unstructured data as applicable.
k) Analyze and understand the structure and semantics of the legacy data to develop an appropriate data migration template.
l) Design the data migration template with basic sanity checks and validation rules to prevent incorrect data entry.
m) Take full responsibility for ensuring that all necessary data sets required for operationalizing the agreed user requirements are successfully migrated to the new system.
n) Coordinate with OCAC for access to existing datasets and manage data extraction, normalization, transformation, and migration in line with the proposed data framework and standards.
o) OCAC shall not bear any responsibility related to the transition or data migration activities, other than facilitating the handover and takeover process between the existing service provider and the new System Integrator (SI)

4.2 Requirement Study

The SI shall perform a detailed assessment of the solution requirements as mentioned in this section. Based on the understanding and its own individual assessment, SI shall develop and finalize the FRS and the SRS in consultation with the OCAC. While doing so, SI at least is expected to do the following:

a) The SI shall liaise with OCAC and other stakeholder Departments
b) The SI shall bring in domain experts during the study
c) The SI shall translate all the requirements mentioned in the document into system requirements
d) The SI shall follow standardized template for requirements capturing
e) The SI must maintain the traceability matrix from SRS stage for the entire implementation

4.3 Design

The SI shall design the solution architecture and specifications for meeting the requirements mentioned as part of this document. The SI shall be entirely responsible for

the design and architecture of the system implemented to satisfy all requirements as described in this document including sizing of the required hardware.

4.4 Development

The SI shall identify, design and develop components / functionalities that are required to address the requirements mentioned in this RFP. The SI shall supply the following documents along with the developed components:

a) Business process guides
b) Data model descriptions
c) Sample reports
d) Frequently asked question (FAQ) guides
e) Any other documentation required for usage of implemented solution

4.5 Integration

a) The SI shall enable integration with different applications and databases (as specified in the below table). The system should support two-way communication with the systems proposed to be integrated.
b) The SI will have to coordinate with the respective teams/departments for integration and OCAC will facilitate this process.
c) The solution should be designed in such a way that any future integration does not require any changes to the system.
d) The solution design should include integration framework for integration of both internal and external applications and services
e) The integration framework should use SOA (Service-oriented architecture) enablement for the underlying applications.

Sl. No	Integration
1	Human Resource Management System (HRMS)
2	Ama Shasana
3	SMS, Email and WhatsApp Integration
4	State Dashboard & SSO
5	OSWAS

Note: This is a tentative integration scope. The actual integration scope will be decided during system study

4.6 Testing

a) The SI shall provide the testing strategy including Traceability Matrix, Test Cases and Conduct Testing of various components of the software developed / customized (e.g. Unit Tests, System Integration Tests, Security Testing and final User Acceptance Test).
b) Details of the testing strategy and approach should be provided in the response.
c) The SI is responsible to identify and inform the OCAC regarding testing requirements and impacts. The SI shall work in a manner to satisfy all the testing requirements and adhere to the testing strategy outlined.
d) SI must ensure deployment of necessary resources, tools, staging servers and related logistics during the testing phases. The SI shall perform the testing of the solution based on the approved test plan, document the results and shall fix the bugs found during the testing.
e) It is the ultimate responsibility of SI to ensure that the end product delivered by the SI meets all the requirements specified in the document.
f) The SI shall take remedial action based on the outcome of the tests.
g) The SI shall provide complete support to the OCAC team or their representatives at the time of user acceptance testing.
h) It would be SI's responsibility to ensure that all issues raised during UAT are closed and signed-off from respective authorities.
i) The SI shall ensure that each module and features developed under this RFP is tested as per the latest version of the IEEE 730 (Software Quality Assurance Processes) standards and shall comply with the latest GIGW guideline.
j) Development, Testing and Staging instance with required infrastructure and software to be provided by SI. Pre-production and production infrastructure are to be provisioned by OCAC at OSDC.

4.7 Third Party Audit

a) The SI needs to ensure that the solution is in compliance with the CERT-In Security Policy and Guidelines.

b) The SI shall appoint CERT-In empaneled auditor who shall be responsible for performing the security audit of the solution.
c) The cost of audit and rectification of non-compliances shall be borne by the SI.
d) Carry out security audit before go-live of the application and obtain the safe-to-host certification.
e) Carry out the periodic audit and certification as and when it is required as per the OSDC policy.
f) The audit shall be performed at least on the below-mentioned aspects.
    i) Functional Testing
    ii) Accessibility Testing
    iii) Application Security Audit
    iv) Vulnerability Testing
g) The illustrative deliverables for this activity are mentioned below:

Activity	Responsibility
First Round Audit Report	Auditor
Rectified solution and submission of next round of audit	SI
Next Round Audit Report	Auditor
Rectified solution and submission of next round of audit, if required	SI
Compliance Confirmation & safe-to-host certificate	Auditor

4.8 SSL Certification

The SI shall carry out SSL certification to ensure :

a) Secure connection between Client and Server through Secure protocol HTTPS
b) Encryption of Data during transmission from server to browser and vice versa
c) Encryption key assigned to it by Certification Authority (CA) in form of a Certificate.
d) SSL Security in the application server

4.9 Training

a) The SI shall provide centralized training to the users of different offices on a train to trainer concept.
b) It would be the SI's responsibility to set up the infrastructure helpful in providing successful training.
c) Infrastructure like computer, network, LCD shall be provided by SI.
d) The schedule/training calendar and the training material for imparting training shall be developed by the SI in consultation with OCAC. The SI shall submit a hardcopy of the training material to OCAC before every training session.
e) In case of modifications either in the training plans or substitutions of the regular trainers, proper correspondence with OCAC shall be made.
f) It is also proposed that the training contents / User Manuals be made available to Users in downloadable (PDF) format so that the Users may refer / download it for their own personal reference as and when needed.
g) It is required that the downloadable training content should have proper indexing and internal references, mapped with key words, in order to allow any User to search and reach the desired content with the help of those keywords

4.10 Deployment and Configuration

a) SI shall deploy the new application/portal over the hardware infrastructure supplied and installed at OSDC.
b) The SI shall be responsible for the end-to-end management of the hosting and deployment of the application.
c) Enterprise grade database shall be provisioned for the proposed application. The SI shall procure required database license for this project in name of OCAC valid for the duration of the project.
d) The SI shall carry out necessary installation, configuration, maintenance & support for the Application production environment and the supplied software(s) as per OSDC policy to ensure that the services are made accessible to the users.
e) The SI shall develop the solution in their own test environment

4.11 UAT and Go-Live

After completion of the development work of Application portal and dashboards, OCAC will conduct the technical reviews of development work performed by the SI as UAT. The SI shall be responsible for:

a) Preparation and submission of test strategy, test cases and test results.
b) Demonstration of module-wise functionalities/ features to designated team in a staging environment.
c) Support OCAC and its designated authority for conducting the testing and provide access of the systems as required by them.
d) Rectification in the database, portal, application for any issues/ bugs/ and improvements/ Enhancements / up-gradations suggested by Departments (if any) during the UAT without any additional cost.
e) After incorporation of the suggestions made during the UAT phase the selected System Integrator shall host the application in the production environment for declaration of Golive.

4.12 Post Implementation Support

The scope of work mentioned under this clause is far beyond the standard maintenance work looking at the number of stakeholders involved.

4.12.1 Application Maintenance

a) Application, System Software Administration & Database cleansing
b) Development/ changes of Form/Report in the developed system
c) Fixing the bugs identified during the period
d) Issue handling and resolution of issues related to application software.
e) Maintaining the updated version of source code
f) Tuning of the system to improve performance
g) Enhancement of MIS report if required
h) User & access management
i) Ensure compliance to SLAs as indicated in this RFP and plan any upgrades / major changes to the software ensuring the SLA requirements are met at no additional cost.
j) Quality audit compliance (if applicable)

4.12.2 System Support

a) Provide integration and user support on all supported servers, data storage systems
b) Manage and monitor hosting infrastructure.
c) Installation and re-installation of the database
d) Handle database installation/re-installation, load balancing, and clustering.
e) Configure networks and perform log analysis (event/system/database).
f) System Administration, Manage database logs, backups, and patch updates.

Apart from the above, the offsite team will also supervise the work of the onsite team as per Software Development Life Cycle (SDLC) process.

4.12.3 Delivery Approach

The selected agency must establish an onsite Operational Support Unit (OSU) with 13 qualified (approximately) resources to ensure effective execution and monitoring of enhancements. The resources will be deployed in 3 locations such as Central PMU, GA&PG Department and CM Grievance Cell.

Skills	No. of Resources	Minimum Educational Qualification and Experience
Team Lead	1	B.E or B.Tech or MCA with minimum 10 years of relevant experience in leading IT teams and managing project delivery. Proven leadership skills, project oversight, coordination, and quality assurance.
Consultant-Technology Management	8	B.E or B.Tech or MCA with minimum 6 years of relevant experience in technology management roles. Strong technical knowledge, hands-on experience in similar system implementation and support activities.
Domain consultant	4	MBA (Marketing) or Mass Communication (Equivalent) with a minimum of 8 years of experience in similar domain consulting roles.

Skills	No. of Resources	Minimum Educational Qualification and Experience
		Expertise in communication, requirement gathering etc.
Support Associates	2	Graduation with a minimum 2 years' experience in Development or Support of IT/ Software Development/ IT System Projects / Website Development / Mobile Application Development.

Note* - *The System Integrator will provide desktop/laptop to the onsite resources and the department shall provide internet connectivity and sitting arrangements for the onsite team. The onsite team shall take necessary guidance as and when required from the department nodal officer for performing their activities.*

5 Functional Requirement for App Modernization

5.1 Technology Upgradation

The SI will do following activities as part of technology enhancement of the existing application

a) Laravel version Upgradation

b) Upgradation to Enterprise based database

c) Architectural level upgradation adopting a microservices-based and multi-layered structure, designed to ensure loose coupling, high availability, fault tolerance, and independent deployment & management of services. The upgraded architecture shall be scalable both vertically and horizontally, enabling individual services/components to scale independently based on demand, and shall incorporate robust security features at all layers.

The overall technology solution shall align with modern Service Oriented Architecture (SOA) principles, implemented through a microservices-based approach, adhering to relevant and suitable industry standards, including standards for service interfaces, API-based integration, XML/JSON services, and necessary protocols for secure internet applications.

5.2 Functional Requirement of New Modules

5.2.1 Government Servants Grievance Page

a) Develop a secure, role-based interface for submitting internal administrative grievances.

b) Ensure data confidentiality and separation from public grievances.

c) Include status tracking, escalation, and redressal features.

d) Enable detailed reporting and performance monitoring.

5.2.2 Reopening of Grievance by Citizen

a) The system shall allow citizens to reopen a grievance that has been marked as “Resolved/Closed” by the concerned authority.

b) The citizen shall be able to access the Reopen Grievance option from the grievance status tracking page available on the web portal and mobile application.

c) The system shall require the citizen to provide mandatory remarks/justification explaining the reason for reopening the grievance.

d) The system shall allow the citizen to upload supporting documents, images, or other relevant evidence while submitting the reopen request.

e) Upon submission, the grievance status shall be automatically updated to “Reopened” in the system.

f) The reopened grievance shall be routed back to the concerned department/authority for further review and necessary action.

g) The system shall maintain a complete audit trail capturing details such as original resolution remarks, citizen’s reopening request, timestamp, and actions taken thereafter.

h) Notifications regarding the reopening request and subsequent updates shall be sent to the citizen through SMS, Email, and other configured communication channels.

i) The system shall allow the department officials to review the reopening request, take further action, and provide updated remarks or resolution.

j) The system shall ensure that the grievance lifecycle, including reopening instances, is reflected in administrative dashboards and MIS reports for monitoring and analysis.

5.2.3 Analytical Dashboard

a) Develop a role-based dashboard for State, District, and Block users.

b) Provide real-time visualizations (charts, graphs, tables) of grievance data.

c) Include KPIs: grievances received/resolved/pending, average resolution time, department-wise performance, escalation rates, and SLA compliance.

d) Support exportable reports (PDF, Excel, etc.).

e) Ensure responsive design, user-friendly navigation, and integration with the core system.

5.2.4 Implementation of AI/ML Capabilities

a) Implementation AI/ML functionalities to enhance automation and intelligence across the grievance lifecycle.

b) Capabilities to include:
   - Severity and Sentiment Analysis: Leverage NLP models to analyze grievance tone and urgency, and auto-assign severity levels for prioritization.
   - Auto-Categorization: Use ML algorithms to classify grievances into predefined and multiple applicable categories.
   - Similar Case Detection: Apply semantic similarity or clustering models to match new grievances with past cases and suggest resolutions.
   - Department Prediction: Implement predictive models to suggest grievances to tag appropriate department/ authorities based on historical patterns.
   - Adaptive Learning: Enable continuous model learning and retraining using new grievance data for improved accuracy over time.

c) Ensure models are explainable, auditable, and periodically updated with new training data.

5.2.5 OCR (Document AI)

a) Deploy OCR to extract structured data from scanned documents, handwritten forms, and images.

b) Auto-fill form fields with key grievance details, citizen info, and metadata.

c) Support multiple Indian languages, including Odia.

d) Ensure compatibility with mobile and web uploads.

e) Seamlessly integrate OCR output into the grievance registration process.

5.2.6 Contextual Search

a) Implement NLP and vector-based search for contextual understanding of grievances.

b) Deliver fast, accurate, and relevance-ranked results beyond keyword matching.

c) Include filters by department, location, type, and time period.

d) Support trend analysis and proactive issue identification.

5.2.7 Object Storage

a) Set up a secure, scalable object storage solution to manage grievance-related files (documents, images, audio, and video).

b) Features should include:
   - Metadata tagging for classification and search.
   - Access control with user-level permissions.
   - Support for high availability, backup, and archival.
   - Integration with existing modules such as OCR, field inspection uploads, and resolution documents.

c) Ensure optimized performance and cost-effective storage management.

5.2.8 AI-Based Chatbot

a) Deploy a 24x7 multilingual chatbot (Odia, English) for grievance registration, status tracking, and FAQs for both Web and Mobile Application.

b) A WhatsApp bot will be developed for grievance registration along with status tracking, FAQs

c) Integrate with the grievance database for real-time responses.

d) Enhance citizen engagement while reducing reliance on human support.

5.2.9 Advisory Module

a) Develop a module to allow departments to issue advisories and standard responses.
b) The module should enable categorization of advisories by department and grievance type.
c) Ensure that advisories are easily accessible to all concerned officers via their dashboards.
d) Provide functionality for version control and expiry of advisories, where applicable.
e) Facilitate better grievance handling through pre-approved policy guidance.

5.2.10 New Feature Addition into Resolution Module

a) Integrate a structured Action Taken Report (ATR) feature.
b) Provide tools for inter-departmental collaboration, including shared notes, comments, and attachments.
c) Implement audit trails to ensure transparency in every step of the resolution process.
d) Require mandatory documentation and remarks before grievance closure.
e) Ensure that closure verification is linked with citizen feedback where applicable.

5.2.11 Enhancement of Mobile Application for Field Inspection Officers

a) Upgrade the mobile app to include Google Maps integration for location tracking and navigation.
b) Allow officers to geo-tag grievance locations, upload inspection media, and record site visits.
c) Enable offline mode for areas with poor network coverage, with automatic sync once reconnected.
d) Provide a structured form for uploading field observations, photos, and reports.
e) Ensure real-time status updates and seamless integration with the central database.

5.2.12 UI/UX Enhancement

a) Redesign the web and mobile interfaces for improved usability and accessibility complying with GIGW and WCAG standards.
b) Support screen readers, Odia language, and intuitive navigation.

c) Introduce intuitive navigation, Odia language improvements, and user-friendly layouts.
d) Implement a responsive design to ensure compatibility with various devices, including low-end smartphones.
e) Include enhancements like tooltips, guided forms, and inline validation for ease of use.

5.3 Security, Integrity & Confidentiality

a) Web Services Security: System shall comply with all the Web services including routing, management, publication, and discovery should be carried out in a secure manner. The Web services should be able to utilize security services such as authentication, authorization, encryption and auditing. Encryption of data shall take place at client level itself. The application server shall provide SSL security.
b) Data Integrity and Confidentiality: Data integrity techniques need to be deployed to ensure that information has not been altered, or modified during transmission without detection. Similarly, Data confidentiality features are also to be applied to ensure that the data is only accessible by the intended parties
c) Transactions and Communications: With respect to the Data Transactions and Communications, the system needs to ensure that the business processes are done properly and the flow of operations are executed in the correct manner.
d) Non Repudiation Security: The application shall have the Non-repudiation security services to protect a party to a transaction against false denial of the occurrence of that transaction by another party.
e) End-to-End Integrity and Confidentiality of Messages: The integrity and confidentiality of messages must be ensured even in the presence of intermediaries.
f) Database Controls: The database controls for online transaction processing shall be enforced such as access to database directly, access to database through application, access to log files, access by the remote terminals, DBA controls, backup policy and backup procedures.

5.4 Change Request Management

During project implementation period it is very usual to find changes in business logic frameworks. In such scenarios, it may be required to develop new software modules beyond the coverage of FRS/SRS/Scope documents, to be considered under Change Request Proposal.

a) Changes in the workflow & any new forms/report of the developed system shall not be considered as Change Request
b) The activities that will be treated as changes request are mentioned below:
    i) Functional changes in the application
    ii) Development/Addition of new modules in the developed system
    iii) Changes in the core application framework
    iv) Integration with any new system
    v) Additional onsite resources in the project
c) The procedure for executing the change request is as follows:
    i) Analysis: The changes suggested shall be analysed by the SI and an effort estimation including timeline shall be submitted to OCAC
    ii) Approval: OCAC shall do the due diligence and provide approval on the effort and timeline suggested
    iii) Incorporation: After receiving the approval from OCAC, SI team will incorporate the changes in the application.
    iv) Payments to such assignment will be as per the man month rate provided in financial bid format and will be made as per actual man month consumed after completion of work of respective enhancement.

5.5 Intellectual Property Rights

The Intellectual Property Rights (IPR) of all software code, data, algorithms, documentation, manuals, digitized documents etc. generated as a part of implementation and O&M of this project shall solely vest with OCAC. The SI will not have any right to share, use or disclose above mentioned components/artifacts. The source code of entire applications along with necessary documentations developed under this RFP/ Contract should be shared with OCAC after Go-live of the application.

5.6 Exit Plan

a) The selected firm will provide a systematic exit plan and conduct a proper knowledge transfer process to handover operations to the OCAC technical team at least three months before project closure.

b) IT resource persons of OCAC will work closely with resource persons of SI at test, staging and production environment during knowledge transfer phase.

c) All knowledge transfer should be documented and possibly recorded.

d) The SI will ensure capacity building of the IT resource persons of OCAC on maintenance of software and infrastructure

6 Project Documentation

The SI will share the below list of deliverables during the project contract period.

a) During Requirement study phase
   i) Project Inception report
   ii) System requirement Study Documents
   iii) Screen prototypes & prototype walkthrough
   iv) High Level Design (HLD)/ Low Level Design (LLD) Including
      - Application architecture documents
      - ER diagrams and other data modeling documents
      - Database design
      - Application component design including component deployment views, control flows, etc.
      - Application flows and logic

b) During Design, Development and Testing Phases
   i) Approved design plan
   ii) Test Plans, Test cases, Test Result

c) Third Party Audit
   i) Report of security audit and Safe- to-Host Certificate

d) Training
   i) User Manual
   ii) FAQ Documents
   iii) Help documents
   iv) Video tutorials
   v) Application Installation & Configuration Manual

e) User Acceptance Test and Go- Live
   i) Leaflet with Infographics & Key highlights
   ii) Audio-visuals(2-3minutes)
   iii) Latest version of Source Code & Database

7 Timeline

The project will initially be for a period of 3 years from the date of go-live of Jana Sunani 2.0. It can be extended for another 2 years based on the requirement and the performance of the System Integrator.

Sl#	Category	Timeline
a)	Takeover & Maintenance and operation Support of the existing application	T0+90 days
b)	System Study and Prototype Design	T0+15 days
c)	Design & Development	T0+60 days
d)	Testing & UAT	T0+ 75 days
e)	Training and Security Audit	T0+85 days
f)	Go-Live of the application	T1= T0+90 days
g)	Application Maintenance Support	36 months from T1
h)	Operational Support Unit	Within 7 days from date of issuance of work order till end of contract

T0 = Date of Letter of Intent /Work Order

Design, Development & Implementation and UAT, Training & Go-Live of the portal are progressive stages of the project. Critical modules must be developed in earlier phases and the deliverable timelines mentioned above are for the finished portal.

8 Service Level & Penalty

The SI shall agree to the following Service Level Agreement (SLA), if it fails to deliver as per scope of work within the corresponding Delivery Period and any extension thereof. These SLAs shall be tracked on the basis of timeline and are envisaged to have penalty and/or liquidation damage clauses on non-adherence to any of them.

Sl #	Service Category	Description	Required Service Level	Penalty
1.	Development & Implementation	Major milestone during development and implementation as per project timeline.	As per project timeline	0.1% of the development cost per day delay
2.	Application availability	Availability of all Modules for at least 99.9% of time measured on monthly basis for a 24x7x365 time period excluding the OSDC network downtimes, if any. The non-availability for application service, website measured on monthly basis and excluding the scheduled maintenance shutdown.	Required 99.9%	Availability & Penalty >=99% & <99.9% : 0.5% >=98% & < 99% : 1% >= 97% & < 98%: 2% (Applicable on Application Support & Maintenance Cost)
3.	Response time for bug fixing	Time taken (after the request has been informed)to acknowledge problem	Within 24 hours from the time the bug is reported.	Rs. 500/- per hour delay (Applicable on Application Support & Maintenance Cost)

Sl #	Service Category	Description	Required Service Level	Penalty
4.	Resolution Time(Only for Bug fixing)	Time taken by the SI to fix the problem	Problems with severity within 48 hours from the time of reporting.	Rs. 500/- per hour delay (Applicable on Application Support & Maintenance Cost)

- Maximum penalty may be capped at 10% of the component cost excluding GST.
- The applications should be available and performing as per functionalities
- Application availability of less than 97% for two consecutive quarters during the O&M phase shall be considered a breach of the Agreement, and OCAC reserves the right to terminate the Agreement.
- In case, the delay is more than 24 weeks and the cause of delay is attributable to Selected Agency, authority reserves right to increase the penalty value and/ or take appropriate action against the bidder such as cancellation of contract, increase of penalty percentage etc.
- Penalty will not be applicable if the delay is not attributable to the agency/ due to force majeure situation or due to OCAC's default. However, in such cases, the Selected agency has to communicate in writing the reason of delay. The decision of the Purchaser in this regard shall be final.
- If at any time during the Contract, the Selected agency encounters conditions impending timely performance of service, then the agency shall promptly notify to OCAC in writing of the fact of the delay and its likely duration along its cause(s). As soon as practicable, after receipt of the agency's notice, OCAC shall evaluate the situation and may at its discretion waive the penalty on the request of the selected bidder.

8.1 Reporting Procedures of SLA

The SI's representative will prepare and distribute Service level performance report in a mutually agreed format by the 10th working day of the completion of each month. The reports will include "actual versus target" Service Level Performance, variance analysis and discussion of appropriate issues or significant events.

8.2 Definitions

a) "Scheduled Maintenance Time" shall mean the time that the System is not in service due to a scheduled activity. The scheduled maintenance time would not be during Working Hour timeframe. Further, scheduled maintenance time is planned downtime with the prior permission.

b) "Scheduled operation time" means the scheduled operating hours of the System for the month. All scheduled maintenance time on the system would be deducted from the total operation time for the month to give the scheduled operation time. The total operation time for the applications within the Primary DC, DR and critical client site infrastructure will be 12 hrs. X 7 days X 12 months.

c) "System downtime" means accumulated time during which the System is totally inoperable within the Scheduled Operation Time.

d) "Availability" means the time for which the services and facilities are available for conducting operations including application and associated infrastructure. Availability is defined as: {(Scheduled Operation Time – System Downtime) / (Scheduled Operation Time)} X 100%

8.3 Interpretations

a) The SLA parameters shall be monitored on a monthly basis as per the individual SLA parameter requirements.

b) The SI is expected to provide the required service levels. In case the service levels cannot be achieved at service levels defined in the tables below, it shall result in a breach of contract and invoke the penalty clause. Payments to the SI are linked to compliance with the SLA metrics.

c) During the contract period, it is envisaged that there could be changes to the SLA, in terms of addition, alteration or deletion of certain parameters, which is based on mutual consent of both the parties i.e. the OCAC and SI.

9 Payment Terms

Sl#	Activity	Milestone/Deliverable	Payment Terms
a)	Takeover and Application Maintenance Support of the existing Jana Sunani Application	Quarterly Activity Report	Quarterly, 100% of the component cost upon approval of activity reports.
b) c)	Study, Design, Development and Implementation of the Enhanced Version of Jana Sunani Web & Mobile Application	• Approval of Software Requirement Specification Document • User Acceptance Test Certificate	60% of the component cost after UAT completion
d)		Go-live Certificate	30% of the component cost after Go-live of application
e)		Leaflet Audio visual	The remaining 10% will be released equally in 4 quarters (1st Year)
f)	Integration with Third-Party Applications	UAT confirmation of data sharing between the applications & Go-live	100% of respective integration cost

Sl#	Activity	Milestone/Deliverable	Payment Terms
g)	Application Maintenance Support of Jana Sunani 2.0	Quarterly Activity Report	Quarterly, upon approval of activity reports.
h)	Third-party Security Audit of Web & Mobile Application	Safe-to-Host Certificate	100% of the audit cost upon submission of Safe-to-Host certificate of respective audit
i)	Project Monitoring Unit	Activity Report	Quarterly, upon approval of activity reports
j)	Change Request – Software Enhancement Service	Go-live	100% of the respective change request cost, upon go live
k)	Database License (Enterprise)	Issue of License in the Name of OCAC	Annually, upon submission of license copy of respective year
l)	Server with OS (Including 3 Year Support)	Delivery Challan	70% of the component cost on delivery. 30% of component cost on Completion of UAT.
m)	GPU Server with OS (Including 3-year Support)	Delivery Challan	70% of the component cost on delivery. 30% of component cost on Completion of UAT.

Sl#	Activity	Milestone/Deliverable	Payment Terms
n)	Any Other Third-Party Tools	Supply and Installation Certified by OCAC	100% of the Tool cost to be paid upon supply and installation

N.B.

i. The SI may propose any third-party tools or licenses required for their proposed solution, except for the Database License. These licenses must be provided by the SI for the entire duration of the project and should be procured in the name of OCAC

ii. The cost associated with SMS, Email, and WhatsApp (including API and tool costs) shall be borne by OCAC.

Note:

i. Payments shall be processed, after successful completion of the target milestones (including specified project deliverables), after submission of an invoice along with supporting documents subject to penalties, if any.

ii. The currency or currencies in which payments shall be made to the SI under this Contract shall be Indian Rupees (INR) only.

iii. In case of disputed items, the disputed amount shall be withheld and will be paid only after settlement of the dispute.

iv. Any penalties/ liquidated damages, as applicable, for delay and non-performance, as mentioned in this document, shall be deducted from the payments for the respective milestones.

v. Taxes, as applicable, will be deducted/ paid, as per the prevalent rules and regulations at the time of billing.

10 Specification of Servers and Enterprise Database

10.1.1 Application server

Sl.	Minimum Requirement Specification	
1	Form factor	Maximum 2U rack mount server with Bezel, Bezel Locking Kit, Chassis Intrusion Detection Kit, and rack-mount kit.
2	Processor	2 no's 5th/higher Gen Intel, 2.1GHz, 32-core, 140MB L3 cache, 64-bit x86 processor fully binary compatible to 64/32-bit applications and supporting hyper-threading. Number of cores on a single die/socket will be treated as a single processor.
3	Memory	1 TB DDR5 RAM in balanced configuration scalable up to 3TB. Minimum 5200 MT/s or higher.
		Advanced ECC to protect servers against single-bit errors as well as to protect against multi-bit memory errors within a single RAM chip as well as within a single memory module.
4	Memory RAS	Adaptive Double DRAM Device Correction (ADDDC), online spare, & mirroring.
5	Storage controller	Tri-mode SAS/SATA/NVMe RAID controller with RAID 1/5/6/10/50/60 support. Offered controller must support mix-and-match up to 8 no's 12G SAS, 6G SATA, and 16G NVMe drives to the same controller.
		Offered Storage controller must support: a) Immutable Hardware root of trust b) Expand & Move Logical Drive c) Configurable stripe size up to 1 MB d) Instant Secure Erase e) Migrate RAID/Stripe Size f) SSD wear gauge. g) Re-enable Failed Logical Drive
6	Disk drives	3 x 1.92TB NVMe SSD.
7	Graphics	Video modes up to 1920 x 1200@60Hz (32 bpp).
8	LAN port	2 x 2-port 25G (SR), 2 x 2-port 32G FC (SW)

9	OS & Hypervisor certification	Certified for latest version of Red Hat Enterprise Linux, SUSE Linux Enterprise Server, Ubuntu, Microsoft Windows Server, HVM, and VMWare.
10	Power supply	Minimum Hot Plug Redundant power supplies of maximum 2kW or better with minimum 94% or better efficiency.
11	Fans/blower	Fully populated redundant (N+1) hot-swap fans system
12	PCI interfaces	Server should have PCIe 5.0 or higher slots.
13	Other interfaces	Minimum 1 x 1Gbps Dedicated OOB system management port (RJ-45), 1 x video port, 4 x USB 3.0/higher ports
14	Driver/ Software Utilities	All required device drivers for OS installation/System Configuration and Server Management. Offered server management software shall be with perpetual licensing.
15	System Compliances	ACPI 6.5, PCIe 5.0, SMBIOS 3.7, UEFI, IPMI 2.0, TPM 2.0, USB 3.2, AES, SNMP v3, TLS 1.2, RESTful API, HTTP/HTTPs Boot, PTT, ASHRAE A3/A4
		Continuous, proactive health monitoring as well as notification of actual or impending component failure alerts on key internal server components such as CPUs, memory, temperature, fans, RAID controllers, hard drives (including cache modules) and power supplies.
16	System BIOS	System should boot with & run the BIOS from the same server hardware OEM (manufacturer). All updates should happen only using quoted OEM's access controller & perpetual management software to enforce security.
17	Server System Security	Immutable Silicon-based Hardware Root of Trust meeting to or exceed FIPS 140-3 or higher. TPM 2.0, CNSA, EAL 4 or higher common criteria certification.
		UEFI Secure Boot & Secure Start, with Continual Runtime Firmware Validation
		One-button/click Secure erase of NAND/user data
		Server should have security dashboard: displaying the status of important security features, the Overall Security Status for the system, and the current configuration for the Security State and Server Configuration Lock features

		Secure recovery or equivalent feature to recover critical firmware to known good state on detection of compromised/malicious firmware.
		Server should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components. Should have dashboard for firmware baselines while performing minimum required firmware checks and highlighting out-of-compliance devices for updates with the selected firmware baseline.
18	System management	System management software should be from the same server hardware OEM. System management software shall be with perpetual license.
		Should provide a Server workload-performance advisor to enable/help in server tuning recommendations to improve server performance
		System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder.
		Server should support monitoring and recording changes in the server hardware and system configuration. It assists in diagnosing problems and delivering rapid resolution when system failures occur
19	Warranty	Three years on-site comprehensive OEM Warranty Support with 24X7 coverage and access to OEM TAC/support. OEM shall have their own support portal to log the case online and historical data about cases must be available in the same portal.
20	IDC Ranking	OEM should be ranked within top 3 as per IDC report for any one of the previous four quarter in India for server.
21	OS	The bidder shall supply the server with Windows/Linux operating system, including a 3-year subscription and round-the-clock (24×7×365) support.

10.1.2 GPU Server

Sl.	Minimum Requirement Specification	
1	Form factor	Maximum 2U rack mount server with Bezel, Bezel Locking Kit, Chassis Intrusion Detection Kit, and rack-mount kit.
2	Processor	2 no's 5th/higher Gen Intel, 2.1GHz, 32-core, 140MB L3 cache, 64-bit x86 processor fully binary compatible to 64/32-bit applications and supporting hyper-threading. Number of cores on a single die/socket will be treated as a single processor.
3	Memory	1 TB DDR5 RAM in balanced configuration scalable up to 3TB. Minimum 5200 MT/s or higher.
		Advanced ECC to protect servers against single-bit errors as well as to protect against multi-bit memory errors within a single RAM chip as well as within a single memory module.
4	Memory RAS	Adaptive Double DRAM Device Correction (ADDDC), online spare, & mirroring.
5	Storage controller	Tri-mode SAS/SATA/NVMe RAID controller with RAID 1/5/6/10/50/60 support. Offered controller must support mix-and-match up to 8 no's 12G SAS, 6G SATA, and 16G NVMe drives to the same controller.
		Offered Storage controller must support: a) Immutable Hardware root of trust b) Expand & Move Logical Drive c) Configurable stripe size up to 1 MB d) Instant Secure Erase e) Migrate RAID/Stripe Size f) SSD wear gauge. g) Re-enable Failed Logical Drive
6	Disk drives	3 x 1.92TB NVMe SSD.
7	Graphics	Video modes up to 1920 x 1200@60Hz (32 bpp). 1 no. NVIDIA A100 40GB GPU.

8	LAN port	2 x 2-port 25G (SR), 2 x 2-port 32G FC (SW)
9	OS & Hypervisor certification	Certified for latest version of Red Hat Enterprise Linux, SUSE Linux Enterprise Server, Ubuntu, Microsoft Windows Server, HVM, and VMWare.
10	Power supply	Minimum Hot Plug Redundant power supplies of maximum 2kW or better with minimum 94% or better efficiency.
11	Fans/blower	Fully populated redundant (N+1) hot-swap fans system
12	PCI interfaces	Server should have PCIe 5.0 or higher slots.
13	Other interfaces	Minimum 1 x 1Gbps Dedicated OOB system management port (RJ-45), 1 x video port, 4 x USB 3.0/higher ports
14	Driver/ Software Utilities	All required device drivers for OS installation/System Configuration and Server Management. Offered server management software shall be with perpetual licensing.
15	System Compliances	ACPI 6.5, PCIe 5.0, SMBIOS 3.7, UEFI, IPMI 2.0, TPM 2.0, USB 3.2, AES, SNMP v3, TLS 1.2, RESTful API, HTTP/HTTPs Boot, PTT, ASHRAE A3/A4
		Continuous, proactive health monitoring as well as notification of actual or impending component failure alerts on key internal server components such as CPUs, memory, temperature, fans, RAID controllers, hard drives (including cache modules) and power supplies.
16	System BIOS	System should boot with & run the BIOS from the same server hardware OEM (manufacturer). All updates should happen only using quoted OEM's access controller & perpetual management software to enforce security.
17	Server System Security	Immutable Silicon-based Hardware Root of Trust meeting to or exceed FIPS 140-3 or higher. TPM 2.0, CNSA, EAL 4 or higher common criteria certification.
		UEFI Secure Boot & Secure Start, with Continual Runtime Firmware Validation
		One-button/click Secure erase of NAND/user data
		Server should have security dashboard: displaying the status of important security features, the Overall Security Status for the system, and the current configuration for the Security State and Server Configuration Lock features

		Secure recovery or equivalent feature to recover critical firmware to known good state on detection of compromised/malicious firmware.
		Server should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components. Should have dashboard for firmware baselines while performing minimum required firmware checks and highlighting out-of-compliance devices for updates with the selected firmware baseline.
18	System management	System management software should be from the same server hardware OEM. System management software shall be with perpetual license.
		Should provide a Server workload-performance advisor to enable/help in server tuning recommendations to improve server performance
		System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder.
		Server should support monitoring and recording changes in the server hardware and system configuration. It assists in diagnosing problems and delivering rapid resolution when system failures occur
19	Warranty	Three years on-site comprehensive OEM Warranty Support with 24X7 coverage and access to OEM TAC/support. OEM shall have their own support portal to log the case online and historical data about cases must be available in the same portal.
20	IDC Ranking	OEM should be ranked within top 3 as per IDC report for any one of the previous four quarter in India for server.
21	OS	The bidder shall supply the server with Windows/Linux operating system, including a 3-year subscription and round-the-clock (24×7×365) support.

10.1.3 Enterprise Database License:

#	Category	Feature Description
1	RDBMS	Enterprise Grade 64 Core
2	License type	Open-source/Commercial with 24×7 enterprise support
3	Deployment Mode	On-Premises
4	Data Storage & Management	Tablespaces, Partitioning (Range/List/Hash), Compression support
5	High Availability (HA)	Streaming Replication, Synchronous/Asynchronous Replication, Failover Manager
6	Scalability	Horizontal read scaling (replica-based), Sharding (via Citus or native partitioning)
7	Performance Optimization	Query planner, Parallel query execution, JIT compilation, Connection pooling
8	Security	Role-based access control (RBAC), LDAP/Kerberos Authentication, SSL/TLS encryption (in-transit), Data-at-rest encryption
9	Backup & Recovery	Point-In-Time Recovery (PITR), WAL Archiving, Incremental Backup, Hot Backup, Logical Backup
10	Disaster Recovery (DR)	Asynchronous replication to DR site, WAL file shipping, Cross-region replication supported