Request for Proposal

Selection of System Integrator for Implementation, Operation & Maintenance of AI Based Solutions for delivery of various G2C Services of Government of Odisha

RFP No.: OCAC-IFITP-PROP-0003-2026-26023

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. Background

The Odisha Computer Application Centre (OCAC), under the Department of Electronics & IT, Government of Odisha, leads the state's e-Governance initiatives. As the government's tech backbone, OCAC drives digital transformation, aiming to enhance public service delivery through ICT. It collaborates with various departments to implement innovative, citizen-centric digital solutions that promote transparency, efficiency, and accessibility across Odisha.

This Request for Proposal (RFP) from qualified Bidder for the development, implementation, operation management, and maintenance of AI-based solution for Odisha government website search and summarization for OCAC and other state departments of Government of Odisha.

Initially, the AI-based website search and summarization solution to be implemented as part of the scope of this RFP will be hosted on cloud services. The engagement of an Bidder to work in collaboration with Bidder who will perform specific activities identified by OCAC for a mentioned period.

Objective

The objective of this RFP is to select a qualified Bidder to design, implement, operate, and maintain AI-based solutions that improve citizen access to government services in OCAC. The project focuses on building an AI-enabled government website search, summarization, and chatbot platform that allows citizens to easily find information across multiple Odisha government websites using text or voice queries.

The solution will also include Generative AI–based enterprise search and AI agents for government employees, enabling them to quickly retrieve policies, documents, and departmental information from various government data sources to improve productivity and decision-making.

Overall, the initiative aims to enhance digital governance by providing a unified, AI-powered interface for citizens and government staff, improving accessibility, efficiency, and responsiveness of public services through OCAC.

2. Scope of Work

2.1. Requirement Study

The Bidder shall perform the detailed assessment of the solution requirements as mentioned in this section. Based on the understanding and its own individual assessment, the Bidder shall develop & finalize the System Requirement Specifications (SRS) in consultation with OCAC. While doing so, the Bidder is expected to do following:

a) The Bidder or shall liaise with OCAC Department officials, Govt. of Odisha.

b) The Bidder shall consult with the domain experts and translate all the requirements mentioned in the document into System Requirements
c) The Bidder shall follow standardized template for requirements capturing
d) The Bidder must maintain traceability matrix from SRS stage for the entire implementation

2.2. Design

a) The Bidder shall be entirely responsible for the design and architecture of the system implemented to satisfy all requirements as described in this document including suggestion on sizing of the required hardware.
b) Bidder shall be responsible for the preparation of System Requirement Specification (SRS) document covering all modules & features planned to be covered as specified based on the outcome of detailed System Study and refined/ improvised FRS.
c) Bidder shall demonstrate the SRS including screen templates, reporting requirements, process flow, and new features suggested for review and shall incorporate all the suggestions / modifications for approval by OCAC/Department.
d) Bidder is required to update the SRS documents as and when any enhancement/ modifications is made into the module/ system till the duration of contract.

2.3. Development

The Bidder shall design and develop the AI based application to address the requirements of OCAC including but not limited to the approved SRS, Solution Architecture & Standards as specified in this RFP document.

2.4. Testing

a) The Bidder shall design the testing strategy including test cases and conduct testing of various components of the solution developed. The solution testing shall at least include Unit Testing, System Integration Testing, Performance Testing, and User Acceptance Testing (UAT).
b) The Bidder shall perform the testing of the solution based on the test plan, document the results, fix the bugs found during the testing and take remedial action based on outcome of the tests.
c) Bidder must ensure deployment of necessary resources, tools and related logistics during the testing phases.

2.5. UAT and Go Live

a. After completion of the development work for application OCAC will conduct the reviews of development work performed by the Bidder as UAT. OCAC may constitute a UAT committee for this purpose.
b. The Bidder shall be responsible for:
    i. Preparation and submission of test strategy, test cases and test results
    ii. Demonstration of module-wise functionalities/ features before the OCAC.
    iii. Support OCAC and its designated authority for conducting the testing and provide access of the systems as required by them.
    iv. Rectification in the new application for any issues/ bugs/ and improvements/ Enhancements / upgradations suggested Departments (if any) during the UAT without any additional cost.
    v. It would be Bidder's responsibility to ensure that all issues raised during UAT are closed and signed off from respective authority

c. After incorporation of the suggestions made during the UAT phase, the Go-live of the system will be declared.

d. After the Go-live, the application will be rolled out for Operation and Maintenance for the given time

2.6. Training & Handholding Support

a) The Bidder is required to undertake training for the end users to make them acquainted with the application.
b) The schedule / training calendar and the training material for imparting training shall be developed by the Bidder in consultation with OCAC. 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
c) The Bidder shall also provide hand-holding support to Department users as required during the contract period and shall deploy necessary resources for a duration of three years from the Go-Live of application.

2.7. Annual Maintenance Support

Support and maintenance will be provided for a period of 3 years from the date of go live of the application including following:

a) Application, System Software Administration
b) Fixing the bugs identified during the period
c) Issue handling and resolution of issues related to application.
d) Maintaining the updated version of application
e) Tuning of the system to improve performance
f) User & access management
g) 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.

2.8. High-level scope of work

The scope of work includes the Development and implementation of the AI-based solution listed in this section of the RFP document. The operation management of the AI-based solution is for a period mentioned in section 2.7 above.

The bidder shall design, develop, and implement an AI-enabled common search interface to enable citizens to easily discover information and services across Odisha Government websites through a unified and intuitive interaction mechanism. The proposed solution shall provide an AI-enabled search and conversational interaction interface capable of understanding natural language queries and providing contextually relevant responses derived from authoritative government sources

The system shall enable citizens to submit queries through text as well as voice input in English, Hindi, and Odia languages. The system should support cross-language search capabilities enabling users to submit queries in supported languages while retrieving relevant information from content available in other languages. Voice inputs shall be converted into text using speech recognition capabilities, and the system shall generate responses in the same language as the user query. The solution shall also support Text-to-Speech (TTS) functionality to convert AI-generated responses into audio format to improve accessibility for users.

The platform shall leverage AI-based semantic search and summarization capabilities to provide clear, structured, and actionable responses to user queries. Responses should present concise explanations along with step-by-step guidance, eligibility criteria, links to relevant forms, and references to official government websites wherever applicable. The system shall display relevant reference links from Odisha Government websites (odisha.gov.in) to allow users to access the original source content and verify the information.

The AI responses shall be generated using content sourced from official Odisha Government websites and relevant Government Orders (GOs) issued by the Government of Odisha, ensuring that the information provided to citizens is accurate, reliable, and traceable to authoritative sources. The system shall include mechanisms for automated content crawling, ingestion, indexing, and periodic updates to ensure that the information repository remains up to date. The platform should also support ingestion of official news feeds and announcements, along with an archival capability to store and retrieve historical information where required. The platform shall support configurable source management allowing authorized administrators to onboard, approve, or remove government websites and knowledge sources.

The solution shall incorporate appropriate AI guardrails to ensure that responses are generated only from approved and indexed government sources. The system should include mechanisms to prioritize authoritative and latest information by leveraging metadata such as publication date, document version, and source credibility. In cases where information from multiple sources appears inconsistent, the system should prioritize the most recent and authoritative source while presenting appropriate references to the original government websites for transparency.

The solution shall be designed using a scalable and modular architecture capable of supporting integration with other citizen engagement platforms. The system should support API-based integration with external channels such as WhatsApp or similar messaging platforms to allow citizens to access the search and information services through additional digital touchpoints.

The platform shall include mechanisms for continuous improvement and governance of the AI system. This shall include the ability to capture citizen feedback on AI-generated responses, such as indicating whether the response was helpful or requires improvement. The system shall also support a human-in-the-loop (HITL) mechanism enabling authorized administrators to review responses, validate knowledge sources, and update the knowledge base where required to improve response accuracy.

The platform shall maintain logs of queries, system responses, and system events for monitoring, troubleshooting, and audit purposes. An administrative analytics dashboard shall be provided to monitor usage patterns and system performance. The dashboard should provide insights such as popular search queries, frequently accessed services, language usage trends, queries that returned low-confidence responses, and queries that returned no results. These insights shall support continuous refinement of the AI system and help government departments identify content gaps and improve the quality, clarity, and accessibility of information published on official government websites.

2.9. Detailed scope of work

2.9.1. Development and implementation of AI-based Solutions

The Bidder will be responsible for the development and implementation of the following AI- based solutions:

2.9.1.1. AI-enabled Government Website Search, Summarization and Chatbot Solution

The scope of work will include the development and implementation of an AI-enabled common search bar for all Odisha government websites of the Odisha Government. The search bar will be designed to:

- Enable citizens to submit queries in text and audio format in English, Hindi, and Odia languages.
- Provide AI-generated responses in the same language as the query, along with an audio format option.
- Provide AI-generated responses in a simple format allowing citizens to understand clearly the actions to be taken to avail services
- Provide AI-generated responses in a structured format guiding citizens with the required step-by-step details and relevant links for actions to be taken not limited to forms to be filled or check their eligibility for a scheme or check status of their application
- Deliver a list of the top relevant reference links from Odisha government websites that pertain to the query.
- Ensure the AI model exclusively utilizes content from Odisha government websites to generate responses.
- Ensure the AI model exclusively utilizes content from Odisha government websites with Latest Government Orders (GOS) from Central and Government of Odisha government to generate responses.
- Ensure the AI model onboards real-time news feeds and sets up an archival system to store and retrieve historical articles for contextual analysis
- Solution should be capable to be integrated with WhatsApp based applications via API

2.9.1.2. Gen AI based employee productivity capability for Enterprise Search and AI agents

The scope would consist of providing a Gen AI enabled Agentic AI for workforce, knowledge workers to leverage the power of Large Language Models and Gen AI and provide a quality search and agents with the highest levels of compliance and data protections for boosting the productivity of the government employees.

The detailed functional and technical specifications for the above solution is mentioned in the subsequent sections of the RFP.

2.9.2. Operation management of implemented solution

The Bidder will be responsible for the operation management and maintenance of the implemented AI-based solution for a period as mentioned in the section 2.7 above from the date of implementation completion. The scope of work includes:
Providing technical support to ensure the smooth functioning and availability of the proposed AI-based solution.

1) Conducting comprehensive user training programs to enable proficient utilization of the AI-based solution by government employees and citizens.
2) Implementing minor platform enhancements to optimize performance and address evolving user requirements.

2.10. Bill of Quantity

AI-based Website Search and Summarization engine with chatbot interface

S No	Items	Quantity
1	AI-based Website Search, Summarization with text and voice enabled chatbot interface with required integrations.	As per functionality
2	Analytics & Reporting on the usage parameters of the proposed solution	As per functionality
3	Required cloud services and storage to operationalize the solution	As per functionality
4	Annual Maintenance Contract	As mentioned in the section 2.7
5	Vulnerability Assessment and Penetration Test	Yearly (Once in a Year)

2.10.1. Gen AI based employee productivity capability for Enterprise Search and AI agents

S No	Items	Quantity
1	Gen AI based solutions should have enterprise search, data connectors and research agents for seamless data discovery and insights for 100 department users. Required licenses and cloud services as required should be suggested as part of the BOQ	As per functionality

2.11. Deliverables

2.11.1. AI-based Website Search and Summarization bar with chatbot interface

Development and implementation of Retrieve Augment and Generate Architecture (RAG) based Website Search and Summarization engine with voice and text enabled bot. The development process should include an AI platform that integrates large language models. These advanced LLMs enhance chatbot performance by retrieving relevant information from a vector database, generating more accurate, factually correct, and contextually appropriate responses based on the government curated datasets.

The deliverables should also include these.

1) Advanced search system using AI to enhance information/ document searchability.
2) Integration with the Odisha government's websites. Government Orders, News feeds
3) Real-time translation, voice command support, and responses using pre-trained models for richer and more intuitive experience like search, Translation, Text-to- Speech, and Speech-to-Text for the search system.
4) User documentation and training materials.

2.11.1.1. Gen AI based employee productivity capability for Enterprise Search and AI agents

The deliverables should be in line with the scope of work mentioned in the RFP and this will include the following:

Provide a Gen AI enabled Agentic AI for workforce which would provide seamless search across all the government data sources with access control to preserve data security.

2.11.2. Cloud Managed Services for AI-enabled Website Search and Summarization with Chatbot Solution and Gen AI based Employee productivity

2.11.2.1. Managed Services

The OCAC department is looking forward to the delivery of the following broad areas of services under this project:

2.11.2.1.1. Design of cloud infrastructure

i) Successful Bidder shall set up and manage the entire cloud solution deployed for department
ii) Provisioning and Managing Cloud based resources on subscription basis .
iii) A successful Bidder shall carry out the capacity planning, accordingly, and on

additional capacity to meet the user growth and/ or the peak load requirements to support the scalability and performance requirements of the solution. There should not be any constraints on the services.

iv) The Cloud services billing shall be done monthly.

2.11.2.1.2. Compliances

a. Bidder shall adhere to the standards published (or to be published) by department or any standards body setup/ recognized by Government of India and notified to the Bidder by department as a mandatory standard.
b. The cloud service offerings of Bidder/CSP shall always remain Empaneled/ complied with the MEITY guidelines and standards. Bidder shall be responsible for the costs associated with implementing, assessing, documenting, and maintaining such Empanelment/Compliances.

2.11.2.1.3. Documentation

i) Bidder shall create and maintain all the necessary technical documentation, design, documents, standard operating procedures, and configurations required to continue operations and maintenance of cloud services.

2.11.2.2. General Requirements

2.11.2.2.1. Self Service Management/ Provisioning

ii) Self Service management/ provisioning focuses on capabilities required to assign services to users, allocate resources, and services and the monitoring and management of these resources.

2.11.2.2.2. User Administration

iii) Bidder shall Implement Identity and Access Management (IAM) that properly separates users by their identified roles and responsibilities, thereby establishing least privilege principles and ensuring that users have only those permissions necessary to perform their assigned tasks.
iv) Bidder shall facilitate Administration of users, identities, and authorizations, effectively managing the root account, as well as any Identity and Access Management (IAM) users, groups, and roles they associated with the user account.
v) Bidder shall Implement multi-factor authentication (MFA) for the root account, as well as any privileged Identity and Access Management accounts associated with it for cloud portal.

3. Technical & Functional Requirement

The Bidder will be responsible for the development and implementation of the following AI-based solutions:

3.1. Functional and Technical Specifications

3.1.1. AI-enabled Website Search and Summarization with Chatbot Solution

In an effort to enhance the quality of public services and improve citizen engagement, the Government of Odisha is aiming to leverage the power of artificial intelligence to provide more efficient, accessible, and responsive services to the citizens of Odisha by providing an AI enabled website search and summarization search bar and chatbot solution for the people of Odisha.

Functional Specifications:

- **User-Friendly Interface:** Provide a search experience where citizens can type or speak their queries in English or Odia.
- **Contextual Responses:** Generate accurate, contextually relevant answers from the content of the websites using LLM model and provide a list of related website links for additional information.
- **Comprehensive Coverage:** Include all the Government of Odisha websites, Government orders, News Articles as mentioned by nodal agency including all the relevant documents in the search database to provide comprehensive search results.
- **Automated Updates and Maintenance:** Implement automated processes for regular updates and maintenance of the search system to ensure ongoing accuracy and relevance of the search results.
- **AI-Generated Response:** Utilize AI to generate concise and relevant responses to the user queries from the content of the Odisha government websites only, enabling users to quickly grasp the key points without reading through extensive documents.
- **Voice Interaction:** Integrate Speech-to-Text cloud services like Speech- to-Text service for capturing user queries through voice commands and Text- to-Speech cloud services like Text-to-Speech service for delivering AI generated response to user queries in audio format, enhancing accessibility for users with different preferences and needs.
- Proposed solution should make best use of a scalable, fully managed multi- modal AI service that processes and understands various data types (text, images, audio) within a single platform, enhancing AI solutions with comprehensive data analysis capabilities.
- Promote Digital Inclusivity: Simplify the process of finding information, making government resources more accessible and user-friendly for all citizens.

Technical Specifications

- Proposed AI based Website search and summarization search bar and chatbot solution should be purpose built and include an AI Platform that leverages the foundational LLM model capabilities for retrieving the relevant and accurate information using vector search-based RAG architecture.
- The proposed solution should have an AI Platform that can leverage foundational multimodal LLM models LLM features to enhance chatbot performance by retrieving relevant information from a vector database, generating more accurate, factually correct, and contextually appropriate responses based on the government curated datasets.
- Proposed solutions should have an AI Platform that support inputs in multiple formats like text or audio for initiating search and should aptly leverage Language Detection and Translation models, Text-to-Speech, Speech-to-Text models in the backend for rendering these features. It is preferred that well tested natural language processing models are used for Translation and Text to Speech and Speech to text pre-trained models.
- The required technology stack should leverage the native CSP services for enabling scalability and high availability for compute, storage and load balancing the web traffic.
- The proposed solution should use the native AI platform services from CSP for foundational LLM models and expose it as an API that can be integrated with the chat application seamlessly.
- The proposed solution should implement an AI-powered search system that delivers real-time, accurate search results from a vast array of government documents, external websites, and PDF files.
- Proposed solution should support multilingual search capabilities in English, Odia, and ensure information is accessible to a diverse population.
- The proposed solution should be based on a semantic search mechanism to perform semantic search, ensuring that the search results are not only based on keyword matching but also on the context and meaning of the user queries.
- Data Encryption: All data should be encrypted in transit and secured against malicious attacks.
- Cloud Platform should be hosted on a MeitY approved cloud provider, the Cloud provider shall meet all MeitY specifications.
- Disaster Recovery, the platform should be able to recover in case of a geographical disaster in one region by falling back to alternate approved infrastructure hosting regions in the MeitY approved cloud provider.

3.1.2. Gen AI based employee productivity capability for Enterprise Search and AI agents

Technical specifications:

- Envisaged solution should provide leading search technology across all an enterprise's data with access control to preserve data security
- Solution should have enterprise connectors and ability to go across enterprise data and applications rather than stay within a single system for surfacing the meaning data spread across multiple data sources.
- Planned Agentic AI solutions should encapsulate all the Enterprise readiness of Cloud: Compliance and regulatory protections such as:
    - Data residency: keeping data and processing within Odisha
    - CMEK: enabling customers to bring their own keys to encrypt their data
    - Audit logging: audit against unauthorized access to data
    - VPC-SC: Restricting the services to within the network perimeter of the customer
    - Responsible AI: Not logging or using any customer data in the services and models and providing responsible AI controls to customers
- Solution should support multi-modal AI features aptly supported by GenAI LLM Models with intrinsic ability to understand images and videos, stream Video and Audio
- The proposed solution should support a research agent feature for extracting key information and help break down complex tasks into manageable steps that are executed in a logical sequence.
- The proposed solution should support integration with E-Office application and must have the capability to automatically ingest E-Office data into Agentic AI solution for AI Processing; build a two-way context bridge for Agentic AI solution can reference E-Office documents and process existing departmental datasets. This integration should also support to write processed summaries, insights, classifications, recommendations to E-Office.

3.1.3. Technical and Functional Compliance for Cloud Services Provider for the Web Site Search, Summarization with Chatbot Solution, Gen AI based Employee productivity

To increase the service availability, the cloud service provider must offer multidimensional auto-scaling of cloud services where resources like RAM and CPU will scale vertically as well systems should scale horizontally

- Cloud service provider should enable the provision of cloud resources through self service provisioning interface.
- Cloud System should enable to provision cloud resources from application programming interface (API)
- Cloud System should be accessible via secure method using SSL certificate.
- Should be able to create, delete, shut down, and reboot virtual machines from Cloud portal.

- Should be able to size virtual machine and select required operating system when provisioning any virtual machines
- Should be able to predict billing of resources before provisioning any cloud resources if integrated with the billing system
- Should be able to set threshold of cloud resources of all types of scalabilities.
- Should be able to provision any kind of resources either static or elastic resources.
- The cloud virtual machine created by the portal should have at-least two virtual NIC cards. One NIC card should be used for internet traffic while another should be used for service traffic.
- The Cloud System shall be capable of allowing applications to self- service compute, network and storage infrastructures automatically based on workload demand.
- Bidder should ensure that the virtual machine format is compatible with other cloud systems.
- Cloud System should give provision to import cloud VM template from other cloud systems.
- Cloud System should support provisioning from self-Cloud Orchestration System to add more storage as and when required by VM.
- Cloud System should give provision to attach new block disk to any cloud VM from self-service portal.
- Cloud virtual machines should be scalable in terms of RAM and CPU automatically without reboot.
- Cloud Systems must support multi-tenancy from a management perspective. Different departments or group companies should be able to access allocated resources only.
- The Solution should provide a simple to use intuitive web end experience for Cloud Administrator and User Departments.
- The Solution should provide Unified Infrastructure management with complete inventory management of virtual machines and physical resources.
- The Solution should provide comprehensive service catalog with capabilities for service design and lifecycle management, and a web- based self-service portal for users to order and manage services.
- Cloud System should have provision to ensure that cloud virtual machine is into a separate network tenant and virtual LAN.
- Cloud System must ensure that cloud virtual machines have private IP network assigned to cloud VM
- Cloud System must ensure that cloud virtual machines have private IP network assigned to cloud VM.
- Cloud System must ensure the ability to map private IP address of cloud VM to public IP addresses as required from the portal of Cloud Orchestration System.
- Should ensure that the cloud VM network is IPV6 compatible.
- Should support use of appropriate load balancers for network request distribution across multiple cloud VMs.

- Cloud Orchestration System should provide network information of cloud virtual resources.
- Cloud Orchestration System should have built-in user-level controls and administrator logs for transparency and audit control
- Cloud Systems should support policy-based provisioning of virtual machines. Based on granted permission, users should be able to perform the operations. For example, if any users don't have permission to delete the VM, he should not be able to do it.
- Cloud Systems should support quota-based systems. Users should not be able to provide resources beyond the allocated quota.
- The admin should be able to define Access Control to Permit or Deny operation per Group or per User.
- Should have provision to define Workflow to Escalate Permission to Group Admins or System Admins.
- The Solution should allow for implementing workflows for provisioning, deployment, Decommissioning all virtual and physical assets in the cloud datacenter.
- User Management: The solution shall provide comprehensive user management
- Functions including tenant-specific user grouping and admin/user rights within the scope of a tenant. The tenant-admin user is considered distinct from the overall cloud solution administrator. The tenant-admin shall be able to manage their own profile, tenant preferences, as well as users within the tenant/group scope. Individual users shall be able to manage their own profile and individual preferences. The solution administrator shall have the right to all User Management functions.
- Cloud System should provide facilities to make templates from virtual machines.
- Cloud System should give provision to make clone of cloud virtual machine from Cloud Orchestration System.
- Cloud System should have provision to live migration of virtual machine to another physical server in case of any failure.
- Cloud System should have provision for migration of virtual machines from one hypervisor platform to another hypervisor platform through its UI.
- Cloud System cloud shall continuously monitor utilization across Virtual Machines and shall intelligently allocate available resources among the Virtual Machines.
- The Cloud System solution shall be able to dynamically allocate and balance computing capacity across collections of hardware resources of one physical box aggregated into one unified resource pool.
- The Cloud System cloud solution should support detecting, in real time, resource requirements of a system in virtual environment and automatic scaling of resource parameters like RAM and CPU to compensate resource requirement in a system.
- The solution should provide near zero downtime host patching with maintenance mode to move running workloads to other hosts on the platform with a consistent audit trail of the patching process.
- Cloud System should give provision to monitor the network traffic of cloud virtual machine.

- Cloud System should offer provision to analyses of amount of data transfer of each cloud virtual machine.
- Cloud System must offer provision to monitor uptime of each cloud virtual machine.
- Cloud System must make provision of resource utilization graphs, i.e., RAM of each cloud virtual machine. There should be provision to set alerts based on defined thresholds. There should be provisions to configure different email addresses where alerts can be sent.
- Cloud System must make provision of resource utilization i.e., CPU graphs of each cloud virtual machine.
- The Cloud System must make provision of resource utilization graphs, i.e., the disk of each cloud virtual machine. There should be graphs of each disk partition and emails should be sent if any threshold of disk partition utilization is reached.
- Cloud System must give provision to monitor the load of Linux/Windows servers and set thresholds for alerts.
- The Cloud System must ensure that there should be historical data of minimum 6 months for resource utilization in order to resolve any billing disputes if any.
- Cloud System must ensure that there are sufficient graphical reports of cloud resource utilization and available capacity
- Should be able to create virtual instances of required configuration without limiting to any standard templates
- Cloud system should natively provide support for Geospatial features including both raster and vector geospatial analysis as part of the cloud offerings
- CSP must only provide OS disks scalable to 64 TB from Day 1 in the Entire Solution, this will be vetted by the Technical Committee.

3.1.4. General Cloud Service Requirement

- Security Monitoring and Posture Management
    - The CSP should have a Managed service for a comprehensive view of the high-priority security alerts and compliance status across multiple accounts.
    - Managed service to provide a single place that aggregates, organizes, and prioritizes the security alerts, or findings, from multiple services and sources.
    - The findings should be visually summarized on integrated dashboards with actionable graphs and tables.
    - CSP should have the capability to continuously monitor the environment using automated compliance checks based on the best practices and industry standards.

- Identity and Access Management
    - CSP should have the capabilities to securely control access to services and resources for the users.
    - CSP should have the ability to create and manage users.
    - CSP should have capabilities to create roles and groups.

  - Support to enforce permission-based access to the resources.
  - Support to manage federated users and their permissions.
- Threat Detection
  - CSP should offer a fully managed threat detection service.
  - Capabilities to continuously monitor malicious or unauthorized behavior.
  - Capabilities to analyze billions of events across multiple accounts using machine learning to detect anomalies.
  - The threat detection service should be able to generate actionable alerts.
  - The threat detection service should support integration with existing event management and workflow systems.
- Security Assessment Services
  - CSP should offer a service for automated security assessment.
  - Service to help improve security and compliance with applications deployed on the cloud.
  - Managed service to automatically assess applications for exposure, vulnerabilities and deviations from best practices.
  - Service should be able to produce a detailed list of security findings prioritized by the level of severity.
  - Should be able to check for unintended network accessibility and vulnerabilities of the VMs.
  - Rules should be regularly updated by the CSP.
- SSL Certificate
  - The CSP should have a service to provision, manage, and deploy Secure Sockets Layer/ Transport Layer Security (SSL/ TLS) certificates.
- HSM
  - CSP should offer fully managed, cloud-based hardware security module to easily generate and use our own encryption keys on the Cloud.
  - The hardware security module should be FIPS 140-2 Level 3 compliant.
  - The hardware security module should support our own encryption keys.
  - The managed hardware security module should support deployment in Single/Multi-tenant mode for high availability.
  - The security module should have the ability to provide high availability and load balancing.
  - Managed hardware security module should have support to integrate with the applications using industry-standard APIs.
- Firewall Management
  - The CSP should offer a security service to centrally configure and manage firewall rules.
  - The security service should be able to configure firewall rules across multiple accounts and applications.
  - The security service should provide a mechanism to easily roll out firewall rules.
  - The security service should be able to support new applications and resources into compliance with a common set of security rules from day one.

  - The security service should provide a single place to build firewall rules, create security policies, and enforce them in a consistent, hierarchical manner.
- Encryption Key Management
  - CSP should offer a fully managed service to create and manage encryption keys.
  - fully managed key management service should be able to control encryption across a wide range of cloud services and applications.
  - The fully managed key management service should be FIPS 140-2 complaint.
  - fully managed key management service should be able to provide the logs of all key usage to help meet our regulatory and compliance.
- Password Management
  - The CSP should have a fully managed service to centrally manage secrets needed to access the applications, services, and IT resources.
  - Fully managed secret management service should be able to easily rotate, manage and retrieve database credentials, API keys, and other secrets throughout their lifecycle.
  - Fully managed secret management service should be able to support API based retrieval of secrets.
  - The fully managed secret management service should be able to control access to secrets using fine-grained permissions.
  - Fully managed secret management service should be able to audit secret rotation centrally for resources in the cloud, third-party services and on-premises.
- DDoS Protection
  - The CSP should have a managed service to protect against Distributed Denial of Service (DDoS) attacks.
  - CSP must provide DDoS Response support provides 24/7 help and potential custom mitigations from DDoS attacks from the same team that protects all services
- Single Sign-On
  - The CSP should have support for Single Sign-On (SSO).
  - The SSO service should be able to centrally manage SSO access to multiple accounts and business applications.
  - The SSO service should be highly available.
  - The SSO service should supportbuilt-in SAML integrations to many business applications.
  - The SSO service should be able to extend SSO access to any of the SAML-enabled applications.
  - The SSO service should be able to use existing corporate credentials to access all the assigned accounts and applications from one place.
- Web Application Firewall
  - The CSP should have a managed web application firewall.
  - The web application firewall should be able to protect the web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources.

  - The web application firewall should be able to give us control over which traffic to allow or block the web application by defining customizable web security rules.
  - The web application firewall should support the creation of new custom rules and block common attack patterns, such as SQL injection or cross-site scripting, OWASP's Top 10 Web Application Vulnerabilities and rules that are designed for our specific application.
  - The web application firewall should be able to deploy new rules immediately.
  - The web application firewall should support API based operations to automate the creation, deployment, and maintenance of web security rules.
- Multi-factor authentication
  - The CSP should offer rule based multi-factor authentication for the cloud portal.
- Automated Vulnerability Management
  - CSP should offer automated vulnerability management service that continually scans virtual machines and container workloads for software vulnerabilities and unintended network exposure.
  - The CSP managed Vulnerability Management Service should automatically detect all newly launched Virtual Machines, and container images pushed to container registry and immediately scans them for software vulnerabilities
  - The CSP managed Vulnerability Management Service should perform automated discovery and continual scanning that delivers near real-time vulnerability findings

3.1.5. Cloud Portal Service Provisioning

- Secured, authenticated and authorized Service APIs to Provision/ Scale/ Manage the resources
- Public Documentation of every API along with examples available in popular programming languages including CLI, Java, Python, Node.js etc.
- Metering and Monitoring of Service usage in terms of compute, bandwidth, storage, performance metrics
- Security by Design: Encryption of data at Rest and while Transit enabled without any manual configuration required. The TLS certificates and Encryptions keys should be secured by Key Management Solution backed by HSM.
- Integration with CSP Identity and Access Management (IDAM) solution to allow granular access control.
- Automated Backup of data with IDAM based Access Control, encryption and monitoring for access/download.
- Automatic Failover without manual intervention.
- Self-Service capability for Restoration of cluster from backup.
- Self-heal capability to detect health of underlying hardware and restore services on a different physical host without any manual intervention.

- Integrated Logging and Monitoring with the option to create alerts based on performance anomaly based on Machine Learning.
- Service version Upgrade with customer having control over the Upgrade window.
- Automated Operating System Patching with customers having control over the Patching window.
- CSP should offer the facility to support Active-Active/Active-Passive architecture having Business continuity plan with built in fault tolerance to avoid any failure at the underlying hardware infrastructure.

3.1.6. Web Application Firewall

- Cloud platform should provide Web Application Filter for OWASP (Open Web Application Security Project) Top 10 protection
- Service provider WAF should be able to support multiple website security.
- Service provider WAF should be able to perform packet inspection on every request covering all 7 layers.
- Service provider WAF should be able to block invalidated requests.
- Service provider WAF should be able to block attacks before it is posted to a website.
- The service provider WAF should have manual control over IP/ Subnet. i.e., Allow or Deny IP/Subnet from accessing websites.
- The attackers should receive custom responses once they are blocked.
- Service providers must offer provision to customize responses to vulnerable requests.
- Service provider WAF should be able to monitor attack incidents and simultaneously control the attacker IP.
- Service provider WAF should be able to Whitelist or Blacklist IP/Subnet.
- Service provider WAF should be able to set a limit to the maximum number of simultaneous requests to the web server and should drop requests if the number of requests exceed the threshold limit.
- The WAF should be able to set a limit to the maximum number of simultaneous connections per IP. And should ban/ block the IP if the threshold is violated.
- WAF should be able to set a limit to maximum file size, combined file size in bytes
- WAF should be able to limit allowed HTTP versions, request content type, restricted extensions and headers
- Service provider WAF should be able to limit the maximum number of arguments, argument name, value, value total length etc.

3.1.7. CSP Native SIEM Solution

- The platform must provide a fully managed Cloud-native SaaS solution from the CSP without any dependency on third parties that requires no maintenance or core monitoring, with systems and security maintained 24x7.

- The platform must offer a seamlessly integrated, advanced SOAR, complete with playbook testing, playbook health monitoring, a comprehensive Integrated Development Environment (IDE), and a diverse marketplace for integrations.
- The platform must include a built-in, integrated User and Entity Behavior Analytics (UEBA) functionality and capability within its SaaS instance of the platform, supporting 3rd party data log sources from various Bidders.
- The platform must support a single integrated SIEM/ SOAR/ UEBA functionalities within a single SaaS application and a single pane of glass.
- The platform must automatically enrich events at data ingestion to enable rapid lookup across multiple large sets of data over a 12-month-old data to achieve:
    - Simpler & Readable Rules and Search Queries
    - Enrichment context which is dynamic & correct with respect to time frame
    - Reduction in table joins/ performance demands
    - Ability to perform historical enrichment for data over 12 months (i.e., user-IP mapping, Geolocation info)"
- The platform must provide embedded hot storage by default for 12 months to cater for extended retroactive search and forensic investigations at no additional cost.
- The platform must have the SIEM/SOAR services delivered specifically in-
- country as a region, as confirmed by publicly available documents.
- The solution must be a cloud-native SaaS application leveraging core Cloud Service Provider (CSP) services in order to ensure maximum resiliency.
- The platform must have a dedicated cloud-native SaaS infrastructure in the country. Core services for both Data at Rest and Data in Transit should be within the country region. If any services are run outside of a country, adequate security mechanisms must be in place to safeguard against unauthorized access, tampering, and modifications.
- The Platform must have Incident Management capabilities for
- coordination during high impact incidents.
- The platform must have the capability to facilitate collaboration with end users externally to the operating organization, enabling them to approve elements of playbook automation and case management.
- The Platform's playbook building must be based on a drag and drop approach with no coding required and includes a Playbook Simulator to test playbooks against production or sample data for validation.
- The Platform must support the creation of bespoke alert views on each playbook for specific SOC roles, ensuring that each SOC role user will see information specific to their needs when performing the investigation.
- The platform must have the capability to support integrating third party intelligence feed

- The solution should come with out-of-the box threat intelligence content and included threat intelligence must be able to be used within threat detection rules.

4. Change Management

Any requirement beyond the scope of work mentioned above shall be treated as Change Request. Change request management shall be conducted based on request received from the Department subject to the approval of the Change Request proposal. The activities that shall be treated as changes request are mentioned below:

- Functional changes in the application
- Development of new modules/Form/Report in the developed system
- Changes in the workflow or core application framework
- Addition of new modules

The procedure for executing the change request is as follows:

- **Analysis**: The changes suggested shall be analyzed and an effort estimation including timeline shall be submitted to the Department.
- **Approval**: Department shall provide approval on the effort and timeline suggested.
- **Incorporation**: After receiving the approval, the changes will be incorporated in the application.
- **Payment**: The additional cost of change requests will be borne by the Department. 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. Exit Plan

a. Bidder shall provide department with a recommended "Exit Management SOP" which shall deal with at least the following aspects of exit management in relation to the SLA as a whole and in relation to the Project Implementation, the Operation and Management SLA and Scope of work definition.
b. Bidder shall provide support to the department for transferring data/ applications at the time of exit management and as per the guidelines defined by MeitY in Cloud Services empanelment RFP.
c. Exit Management Plan will include the following but limited to:
    a. A detailed program of the transfer process that could be used in conjunction with a Replacement Bidder including details of the means to be used to ensure continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer.
    b. Plans for communication with such of the Bidder, staff, suppliers, customers and any related third party as are necessary to avoid any material detrimental impact on Project's operations as a result of undertaking the transfer.
    c. Transition methods include roles and responsibilities of both the parties to handover and takeover the charge of project regular activities and support system.

d. Proposal for necessary set up or institution structure required at department level to effectively maintain the project after contract ending.
e. Training and handholding of department Staff or designated officers for maintenance of project after contract ending.

5.1. Transition-Out Services

a. Continuity and performance of the Services at all times including the duration of the agreement and post expiry of the Agreement is a critical requirement of the department. It is the prime responsibility of Bidder during exit management period and in no way any facility/ service shall be affected/degraded. Further, Bidder is also responsible for all activities required to train and transfer the knowledge to department (or representative agency of department).
b. The exit management period starts, in case of expiry of contract, at least 3 months prior to the date when the contract comes to an end or in case of termination of contract, on the date when the notice of termination is sent to the Bidder. The exit management period ends on the date agreed upon by department or Three months after the beginning of the exit management period, whichever is earlier.
c. At the end of the contract period or upon termination of contract, Bidder is required to provide necessary handholding and transition support to ensure the continuity and performance of the services to the complete satisfaction of department.

6. Project Documentation

Bidder shall create and maintain all the necessary technical documentation, design, documents, standard operating procedures, and configurations required to continue operations and maintenance of cloud services and share with OCAC.

7. Project Timeline

The project shall initially be for a period of 3 years from the date of go-live and Operation & Maintenance may be taken up for another two (2) years based on performance and requirement of the Department.

T0- Issuance of Work Order/Purchase Order

Sl. #	Project Component	Tentative Deliverables	Timeline
1.	Issuance of Work Order to successful Bidder	• Approval letter	T0
2.	Provisioning of Cloud resources	• Access to cloud resources and environment credentials	T0 + 15 days = T1

Sl. #	Project Component	Tentative Deliverables	Timeline
3.	Design and Development of Gen AI-based employee productivity capability for Enterprise Search and AI Agents and AI-enabled Website Search and Summarization with Chatbot Solution	• System Architecture and Design Document approved by the Department • Finalized and approved list of government websites and data sources for content crawling and indexing • Deployment/Hosting of the application in the designated environment	T1 + 120 days = T2
4.	System Integration & Testing	• Test Plans • Test Cases • System Testing Reports	T2 + 30 days = T3
5.	Security Testing (VAPT)	• Vulnerability Assessment and Penetration Testing (VAPT) Report • Closure of identified vulnerabilities	T3 + 10 days = T4
6.	User Acceptance Testing (UAT) & Production Readiness	• UAT Completion Report • Implementation and closure Of UAT observations and feedback • Approval for Production Rollout	T4 + 15 days= T5
7.	Training	• Training sessions for stakeholders • User and Administrator Manuals • FAQs and Knowledge Documentation	T5 + 7 days = T6
8.	Go-Live	• Production rollout approval from the Department • Production Deployment	T6 + 7 days= T7
9.	Operation and Maintenance for 3 years	• Monthly activity reports • Performance monitoring, • Knowledge base updates	36 Months from the date of Go-Live

7.1. Team Structure

Composition and qualification of Managed Service Provider (successful bidder) team for Projection Execution:

S.No.	Position	Qualification and Experience Required	Location
1	Project Manager- 1 No.	a) B.Tech/ BE b) Total 10 years of experience out of which 04 Years of experience must be in the role of Project Management.	On-Site

		Resume to be submitted	
2	Solution Architect – 1 No.	a) B.Tech/B. E. b) 08 Years of experience in role of System Architecture and Software Development. Resume to be submitted	Onsite during Development Period
3	Lead Data Scientist-1 No.	a) B.Tech/B. E. b) Total 06 Years in the role of Data Science. Resume to be submitted	Remote
4	Data Scientist- 1 No.	a) B.Tech/B. E. b) Total 02 Years in the role of Data Science. Resume to be submitted	Remote
5	Back End Developer-1 No.	a) B.Tech/B. E. in IT/CS or MCA b) 3 years' Experience of back-end development. Resume to be submitted	Remote
6	Front End Developer-1 No.	a) B.Tech/B. E. in IT/CS b) 3 years' experience of front-end development. Resume to be submitted	Remote
7	Testing Engineer-1 No.	a) B.Tech/B. E. b) 2 years of Experience. Resume to be submitted	Remote

Note: OCAC will have the right to ask for additional Team members beyond what has been specified in this RFP as per the mutually agreed terms and conditions between both the parties.

8. Service Level & Penalty

8.1. Penalty Terms for Quality of Services

- For the Department to ensure that the successful Bidder adhere to the Service Level Agreements, this section describes the Penalties which may be imposed on successful Bidder. In case these service levels cannot be achieved at the service levels defined in the agreement, the departments will invoke the performance related penalties.
- The penalty in the percentage of the monthly payment has been as indicated against each SLA parameter in the table.

- If outage is due to successful Bidder except application related malfunction, then 10% penalty of month bill will be imposed.
- Payments to be linked to the compliance with the SLA metrics laid down in the agreement. To illustrate calculation of penalties, an indicative example is provided below.
- For ex: For SLA1 if the penalty to be levied is 7% then 7% of the Monthly Payment is deducted from the total of the Monthly bill and the balance paid to the successful Bidder.
- If the penalties are to be levied in more than one SLA, then the total applicable penalties are calculated and deducted from the total of the Monthly bill and the balance paid to the successful Bidder.
- For ex: SLA1 = 7% of the Monthly Payment, SLA12 = 10% of the Monthly Payment, SLA19 = 2% of the Monthly Payment then, Amount to be paid = Total Monthly bill – {(19% of the Monthly Payment)}
- Provide a robust, fault-tolerant infrastructure with enterprise-grade SLAs with an assured uptime of 99.5%, SLA measured at the VM Level and SLA measured at the Storage Levels.
- The SLA for availability of Cloud service (defined as availability of all servers, storage and supporting DC infrastructure including network infrastructure and network connectivity) is 99.5% with no unscheduled downtime. (Total contracted minutes in a quarter – downtime during contracted minutes) * 100 / Total contracted minutes in a quarter
- In case a service provider fails to achieve compliance level of services successively in two quarters or any three quarters in a year, department will reserve the right to re- look at the contract and redefine Service level agreement and penalty clauses to safeguard its interest.

8.2. Billing & Discounting Model

- The price quoted by the Bidder for each line item in the commercial bid format will be frozen for entire contract period.
- The billing for each line item should be calculated either based on the quoted price or the current public pricing (after applying discount), whichever is lower as on billing date.
- The Bidder should provide the discount percentage on each category as mentioned in Bill of Quantity. These discounts would remain firm for the entire contract period.
- The Discount provided as part of this bid document will be used to procure any additional service or configuration of service in the host of offerings of the CSP at the same rate of discount. The services used which do not belong to any category A, B and C, the discount will be calculated based on the category "D".
- To facilitate evaluation of bids, OCAC, at its sole discretion, may seek clarification in writing regarding the bid.
- The department may review the price/cost quoted periodically in view of various factors including but not limited to significant price/cost reduction for same services in market.
- Final choice of firm for the project shall be made on the basis of conformity to eligibility, technical proposal and appropriateness of the financial offer from the point of view of cost effectiveness over the entire period for the services and capability of the firm to execute and service the project.

8.3. Service Level Agreement

- The purpose of Service Levels is to define the levels of service provided by the ("successful Bidder") to the Department for the duration of the contract. The benefits of this are:
    - Help the Client control the levels and performance of successful Bidder's services.
    - Create clear requirements for measurement of the performance of the system and help in monitoring the same during the Contract duration.
- The Service Levels are between the Department and successful Bidder.

8.4. Service Level Agreements and Targets

- This section is agreed to by Client and successful Bidder as the key performance indicator for the project.
- The following section reflects the measurements to be used to track and report system's performance on a regular basis. The targets shown in the following tables are for the period of Contact.

8.5. General Principles of Service Level Agreements

- Service Level Agreement (SLA) shall become the part of the Contract between the Client and the successful Bidder. SLA defines the terms of successful Bidder's responsibility in ensuring the timely delivery of the services and the correctness of the services based on the agreed performance indicators as detailed in this section.
- The successful Bidder shall comply with the SLAs to ensure adherence to project quality and availability of services throughout the duration of the Contract. For the purpose of the SLA, definitions and terms as specified in the document along with the following terms shall have the meanings set forth below:
    - **"Total Time"** – Total number of hours in the quarter being considered for evaluation of SLA performance.
    - **"Downtime"** – Time period for which the specified services/ components/ system is not available in the concerned period, being considered for evaluation of SLA, which shall exclude downtime owing to Force Majeure and reasons beyond control of the successful Bidder.
    - **"Scheduled Maintenance Time"**– Time period for which the specified services/components/system with specified technical and service standards are not available due to scheduled maintenance activity. The successful Bidder shall seek at least 15 days' prior written approval from the Client for any such activity. The scheduled maintenance shall be carried out during non-peak hours and shall not exceed more than four (4) hours and not more than four (4) times in a year.
    - **"Uptime"** – Time period for which the specified services are available in the period being considered for evaluation of SLA.
    - **Uptime (%)** = (1- {[Total Downtime]/ [Total Time- Scheduled Maintenance Time]}) * 100. Penalties shall be applied for each criterion individually and then added together for the total penalty for a particular quarter
    - **"Incident"** – Any event/abnormalities in the service/system being provided that may lead to disruption in regular/normal operations and services to the end user.
    - **"Response Time"** – Time elapsed from the moment an incident is reported to the Helpdesk either manually or automatically through the system to the time when a resource is assigned for the resolution of the same.
    - **"Resolution Time"** – Time elapsed from the moment incident is reported to the Helpdesk either manually or automatically through system, to the time by which the incident is resolved completely and services as per the Contract are restored.

- **"Target"** – is the availability of cloud and managed services and their data. It is calculated as = [(Total uptime of all cloud and managed services in a quarter)/ (Total time in quarter)] *100.
- **Latency:** Latency may address the storage and the time when the data is placed on mirrored storage.
- **Maximum Data Restoration Time:** refers to the committed time taken to restore cloud service customer data from a backup.
- **Recovery Point Objective:** It is the maximum allowable time between recovery points. RPO does not specify the amount of acceptable data loss, only the acceptable time window. RPO affects data redundancy and backup.
- **Recovery Time Objective:** It is the maximum amount of time a business process may be disrupted, after a disaster, without suffering unacceptable business consequences. Cloud services can be critical components of business processes.
- Availability of Reports (Reports such as Provisioning, Utilization Monitoring Reports, User Profile Management etc.)
- Penalty shall be applied for each criterion individually as per downtime of each applicable component and then added together for the total penalty for a particular quarter.

8.6. Service Levels Monitoring

- The Service Level parameters shall be monitored on a quarterly basis. Penalties associated with performance for SLAs shall be made after deducting from applicable payments of the quarter or through the Performance Bank Guarantee.
- As part of the Project requirements, successful Bidder shall supply and make sure of appropriate system (software/hardware) to automate the procedure of monitoring SLAs during the course of the Contract and submit reports for all SLAs as mentioned in this section. This software along with any system specific software shall be used by the successful Bidder for monitoring and reporting these SLAs. The Client reserves the right to test and audit these tools for accuracy and reliability at any time. If at any time during the test and audit the accuracy and reliability of tools shall be found to be compromised, the Client reserves the right to invoke up to double the penalty of the respective quarterly phase.
- The successful Bidder will endeavor to exceed these levels of service wherever possible.
- Successful Bidder undertakes to notify the Client of any difficulties, or detrimental/adverse findings as soon as possible once they are identified.
- Success Bidder will provide a supplemental report on any further information received, as soon as the information becomes available.
- Successful Bidder will take instruction only from authorized personnel of the Client.
- In case issues are not rectified to the complete satisfaction of Client, within a reasonable period of time defined in the RFP, the Client shall have the right to take appropriate remedial actions including liquidated damages, applicable penalties, or termination of the Contract.
- For issues i.e., breach of SLAs beyond control of the successful Bidder, the successful Bidder shall submit a justification for the consideration of the Client. In case it is established that the successful Bidder was responsible for such breach, the respective penalty shall be applied to the successful Bidder.
- In case if any of the information mentioned in the further measurements of services does not match the SLA as per MeitY, then the SLA measurements mentioned in the MeitY guidelines will be final.

8.7. Measurements and Targets – Operations Phase SLAs

- These SLAs should be used to evaluate the performance of the services post the Implementation Phase and during the operations Phase. These SLAs and associated performance shall be monitored on a quarterly basis. Penalty levied for non-performance as per SLA shall be deducted through subsequent payments due from the Client or through the Performance Bank Guarantee.
- The Scheduled Maintenance Time shall be agreed upon with the Client as per the definition given as part of this section of the Contract.
- Successful Bidder's published SLAs and penalties shall also be applicable during the course of the Contract.
- The following SLAs apply both for successful Bidder and successful Bidder/SI. While the successful Bidder will be responsible for maintaining the SLAs pertaining to the cloud infrastructure, network, controls etc., the successful Bidder will be responsible for the SLAs related to managing and monitoring the cloud services

#	Service Level Objective	Measurement Methodology	Target Service / Level	Penalty (Indicative)
Availability/ Uptime				
1	Availability/ Uptime of cloud services Resources for Production Environment (VMs, Storage, OS, VLB, Security Components)	Availability (as per the definition of the SLA) will be measured for each of the underlying components (e.g., VM, Storage, OS, VLB, Security Components) provisioned in the cloud.	Availability for each of the provisioned resources: >=99.5%	Default on any one or more of the provisioned resources will attract penalty as indicated below. =<99.5% - >=99% (10% of the <MP>) < 99% (30% of the <MP>)
2	Availability of Critical Services (e.g., Register Support Request or Incident; Provisioning/ De-Provisioning; User Activation/ Deactivation; User Profile Management; Access Utilization Monitoring Reports)	Availability (as per the definition in the SLA) will be measured for each of the critical services over both the User/ Admin Portal and APIs (where applicable)	Availability for each of the critical services over both the User / Admin Portal and APIs (where applicable) >= 99.5%	Default on any one or more of the services on either of the portal or APIs will attract penalty as indicated below. =<99.5% - >=99% (10% of the <MP>) < 99% (20% of the

	over User/ Admin Portal and APIs (where applicable)			<MP>)
3	Availability of the network links at DC	Availability (as per the definition in the SLA) will be measured for each of the network links provisioned in the cloud	Availability for each of the network links: >= 99.5%	Default on any one or more of the provisioned network links will attract penalty as indicated below. =<99.5% - >=99% (10% of the <MP>) < 99% (30% of the <MP>)
4	Availability of Regular reports (e.g., Audit, Certifications,) indicating the compliance to the Provisional Empanelment Requirements.		15 working days from the end of the quarter. If STQC issues a certificate based on the audit, then this SLA is not required.	5% of MP
Support Channels – Incident and Helpdesk				
5	Response Time	Average Time taken to acknowledge and respond once a ticket/incident is logged through one of the agreed channels. This is calculated for all tickets/ incidents reported within the reporting month.	95% within 15 minutes	<95% and >=90%(5% of the MP) < 90% and >= 85% (7% of the MP) < 85% and >= 80% (9% of the MP)
6	Time to Resolve – Severity 1	Time taken to resolve the reported ticket/incident from the time of logging.	For Severity 1, 98% of the incidents should be resolved within 30 Minutes of problem reporting	<98% and >=90% (5% of the MP) < 90% and >= 85% (10% of the MP) < 85% and >= 80%

				(20% of the MP)
7	Time to Resolve – Severity 2, 3	Time taken to resolve the reported ticket/incident from the time of logging.	95% of Severity 2 within 4 hours of problem reporting and 95% of Severity 3 within 16 hours of Problem reporting	<95% and >=90% (2% of the MP) < 90% and >= 85% (4% of the MP) < 85% and >= 80% (6% of the MP)
Security Incident and Management Reporting				
8	Percentage of timely incident report	Measured as a percentage by the number of defined incidents reported within a predefined time (1 hour) limit after discovery, over the total number of defined incidents to the cloud service which are reported within a predefined period (i.e., month). Incident Response – successful Bidder shall assess and acknowledge the defined incidents within 1 hour after discovery.	95% within1 Hour	<95% and >=90% (5% of the MP) < 90% and >= 85% (10% of the MP) < 85% and >= 80% (15% of the MP)
9	Percentage of timely incident resolutions	Measured as a percentage of defined incidents against the cloud service that are resolved within a predefined time limit (month) over the total number of defined incidents to the cloud service within a predefined period. (Month). Measured from Incident Reports	95% to be resolved within 1 hour	<95% and >=90% (5% of the MP) < 90% and >= 85% (10% of the MP) < 85% and >= 80% (15% of the MP)
10	Percentage of timely vulnerability	The number of vulnerability corrections performed	99.95%	>=99% and <99.95% (10% of

	corrections	by the cloud service provider – Measured as a percentage by the number of vulnerability corrections performed within a predefined time limit, over the total number of vulnerability corrections to the cloud service which are reported within a predefined period (i.e., month, week, year, etc.).		the MP) >=98% and <99% (20% of the MP) <98% (30% of the MP)
11	Percentage of timely vulnerability reports	Measured as a percentage by the number of Vulnerability reports within a predefined time limit, over the total number of vulnerability reports to the cloud service which are reported within a predefined period (i.e., month, week, year, etc.).	99.95%	>=99% and <99.95% (10% of the MP) >=98% and <99% (20% of the MP) <98% (30% of the MP)
Vulnerability Management				
12	Security breach including Data Theft/ Loss/ Corruption	Any incident wherein, system compromised or any case wherein data theft occurs (including internal incidents)	No Breach	For each breach/data theft, penalty will be levied as per following criteria. Any security incident detected INR << 5 Lakhs>>. This penalty is applicable per incident. These penalties will not be part of overall SLA penalties cap per month. In case of serious breach of security wherein the data is stolen or corrupted, Government. Department reserves the right to terminate the contract
13	Availability of SLA reports covering all		(e.g., 3 working days from the	5% of MP

	parameters required for SLA monitoring within the defined time		end of the month)	
14	Availability of Root Cause Analysis (RCA) reports for Severity 1 and 2		Average within5 Working days	5% of MP

Note: MP means Monthly Payment Share of that quarter

8.8. Severity Level

Below severity definition provides scenarios for incidents severity.

Severity Level	Description
Severity 1	More than 50% of users affected for more than one hour
Severity 2	More than 25% and upto 50% users affected for more than 2 hours
Severity 3	Upto 25% of users affected for more than 4 hours.

9. Payment Terms

9.1. Payment Schedule

The payment as specified in this RFP by Selected Bidder shall be made as per the norms.

- The Selected Bidder shall be entitled to receive the Service Charges as per their quotation submitted in Financial Bid.
- The payment to the Selected Bidder will be made on a One Time and Monthly basis. The Service provider has to raise bill for a Month within 10th day of every subsequent Month accompanied by automated system generated performance report mentioning performance achieved in the month against all type of "Service Level Performance" and related LDs.
- Payment will be made for four components during O&M Phase.
    - For Services towards "Web Site Search, Summarization with Chatbot Solution" undertaken in a month at rate of "awarded price" minus all the

LDs combined.

- For Services towards "Gen AI based employee productivity tool" undertaken in a month at rate of "awarded price" minus all the LDs combined

- Apart from the above, below is the payment schedule against one time setup of required application, cloud setup etc.

Sno	Parameter	Payment in % Percentage
Cloud Setup & Provisioning (C1)		
1	Configuration of VMs on Cloud Environment for C2 and C3	70% of One Time Cost for Setup of Cloud Setup & Provisioning (C1)
2	Application Hosting on Cloud for C2 and C3	Remaining 30% of One Time Cost for Setup of Cloud Setup & Provisioning (C1)
Development, Integration and Deployment Website Search, Summarization with Chatbot Solution (C2)		
1	Requirement Gathering & Signoff, D	30% of One Time Cost for C2
2	Design & Development, Integration, Deployment and Go Live for an additional 100 departmental websites	30% of One Time Cost for C2
3	Design & Development, Integration, Deployment and Go Live for an additional 200 departmental websites	20% of One Time Cost for C2
4	Final UAT Signoff for all 400 websites	10% of One Time Cost for C2
5	Final Go-Live of all 400 websites	10% of One Time Cost for C2
Gen AI based Employee productivity capability for Enterprise Search and AI Agents (C3)		
1	Setup of AI based Employee productivity capability for Enterprise Search and AI Agents (100 Licenses and 10 Agents)	70% of One Time Cost for C3

2	Go-Live	30% of One Time Cost for C3
Others		
1	Security Audit	As per actual upon submission of safe to host certificate
2	Application Support and Software Maintenance for a period of three year.	Quarterly payment

General Conditions

a. Payment schedule - Payments to the bidder/authorized partner, after successful completion of the target milestones (including specified project deliverables), would be made as under: -

i. The selected bidder's request for payment shall be made to the purchaser in writing, accompanied by invoices describing, as appropriate, the goods delivered and related services performed, and by the required documents submitted pursuant to general conditions of the contract and upon fulfilment of all the obligations stipulated in the Contract.

ii. Due payments shall be made promptly by the purchaser, generally within thirty (30) days after submission of an invoice or request for payment by the supplier/ selected bidder/authorized partner, and the purchaser has accepted it.

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

c. All remittance charges will be borne by the supplier/ selected bidder/authorized partner.

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

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

f. Taxes, as applicable, will be deducted/ paid, as per the prevalent rules and regulations at the time of billing. Legitimate payment shall be made within 30 working days of the receipt of invoice along with supporting documents subject to penalties, if any.