UNITED INDIA INSURANCE COMPANY LIMITED
Registered Office: 24, Whites Road Chennai - 600014
CIN: U93090TN1938GOI000108

REQUEST FOR PROPOSAL

PROPOSAL FOR SELECTION OF VENDOR FOR ONBOARDING SYSTEM INTEGRATOR (SI) TO IMPLEMENT ENDPOINT SECURITY TOOLS.

United India Insurance Company Ltd. invites bids for Implement Endpoint Security Tools. The details of scope are mentioned in the RFP document. Any change in the below mentioned timelines will be communicated through corrigendum on the website of the company.

Tender No.: 000100/HO IT/RFP/282/2025-2026

Bidders are advised to study this tender document carefully. Submission of bid shall be deemed to have been done after careful study and examination of the tender document with full understanding of its implications. The response to this tender should be full and complete in all respects. Incomplete or partial bids shall be rejected. The Bidder must quote for all the items asked for, in this tender.

The Bidder shall bear all costs associated with the preparation and submission of the bid, including cost of presentation and demonstration for the purposes of clarification of the bid, if so desired by UIICL. UIICL will in no case be responsible or liable for those costs, regardless of the conduct or outcome of the bidding process.

1. Table of Contents

2. INTRODUCTION

United India Insurance Company Limited (UIIC) is a leading Public sector General Insurance Company transacting General Insurance business in India with Head Office at Chennai, with 30 Regional Offices, 6 LCB's and 1300+ Operating Offices geographically spread throughout India. United India Insurance Company Limited, hereinafter called "UIIC" or "The Company", which term or expression unless excluded by or repugnant to the context or the meaning thereof, shall be deemed to include its successors and permitted assigns, issues this bid document, hereinafter called Request for Proposal or RFP.

2.1. PURPOSE OF THIS DOCUMENT

- United India Insurance Company Ltd invites bids (Technical bid and Commercial bid) from eligible bidders for System Integrator (SI) for implementing Endpoint Security Tools as per requirements mentioned in the RFP. This invitation of Bids is open to all System Integrators (SIs) having presence in India, provided bidders fulfill the minimum qualification criteria as mentioned in bid document.
- This RFP contains details regarding the scope, project timelines, evaluation process, terms and conditions as well as other relevant details, which the Bidder needs to factor in while responding to this RFP.

- The scope includes the following Endpoint Security Tools:
  - Data Loss Prevention (DLP),
  - Endpoint Detection and Response (EDR),
  - Data discovery and Data classification,
  - Mobile Device Management (MDM) for laptops and tablets,
  - Patch Management Solution,
  - Key Management Solution for BitLocker keys

2.2. DEFINITION OF TERMS USED IN THIS DOCUMENT

Company/UIIC/purchaser	United India Insurance Limited
RFP	Request for Proposal
SI	System Integrator
OEM	Original Equipment Manufacturer
SLA	Service Level Agreement
BG	Bank Guarantee
EMD	Earnest Money Deposit
MTTR1	Mean Time to Respond
MTTR2	Mean Time to Resolve
INR / Rs	Indian Rupee
POC	Proof of Concept
BOM	Bill of Materials
DC	Data Center (Mumbai)
DR	Disaster Recovery Site (Hyderabad)
NDR	Near Data Center (Mumbai)
HO	Head Office
MAF	Manufacturer's Authorization Form
LAN	Local Area Network
NOC	Network Operation Centre
SOC	Security Operation Centre
QoS	Quality of Service
WAN	Wide Area Network
P2P	Point to Point
ILL	Internet Leased Line
RCA	Root Cause Analysis
AMC	Annual Maintenance Contract
ATS	Annual Technical Support
SOW	Scope of Work
T&C	Terms and Conditions
TCO	Total Cost of Ownership
EOL	End of Life

Company/UIIC/purchaser	United India Insurance Limited
EOS	End of Support
BIA	Business Impact Assessment
PO	Purchase Order
NDA	Non-Disclosure Agreement
FMS	Facility Management Services
L1 Resource	First-level support engineer
L2 Resource	Second-level (advanced) support engineer
DLP	Data Loss Prevention
EDR	Endpoint Detection and Response
MDM	Mobile Device Management
KMS	Key Management Solution
RBAC	Role-Based Access Control
SIEM	Security Information and Event Management
PAM/PIM	Privileged Access Management / Privileged Identity Management
OCR	Optical Character Recognition
API	Application Programming Interface
GUI	Graphical User Interface
HTML5	Hypertext Markup Language version 5
GeoIP	IP-based geographic location identification
ITSM	IT Service Management

2.3. Due Diligence

The Bidders are expected to examine all instructions, terms and specifications stated in this RFP. The Bid shall be deemed to have been submitted after careful study and examination of this RFP document. The Bid should be precise, complete and in the prescribed format as per the requirement of this RFP document. Failure to furnish all information or submission of a bid not responsive to this RFP will be at the Bidders' risk and may result in rejection of the bid. The decision of UIIC on rejection of bid shall be final.

2.4. Eligibility Criteria

#	Eligibility Criteria for Bidders	Documentary Proof Required
1	The Bidder should be a Registered Company in India under the 'Companies Act' and should be in business in India for more than ten years as on 31.03.2025.	Copy of the Certificate of Incorporation issued by Registrar of Companies.
2	The bidder should have an average annual financial turnover of at least ₹500 Crore for the last three financial years' viz. 2021-2022, 2022-2023, and 2023-2024. For startups and MSMEs, the average annual financial turnover should be at least ₹50 Crore for the last three financial years' viz. 2021-2022, 2022-2023, and 2023-2024.	Audited financial statements / Certificate from Auditor.
3	Bidder must have net profit in any of the two years during the last three completed financial years - 2021-2022, 2022-2023, and 2023-2024.	Audited financial statements / Certificate from Auditor.
4	The bidder should not have been blacklisted/ debarred by any Government Departments, Agencies or Public Sector Undertakings in India as on the date of submission of the tender.	As per Annexure 2: No Blacklist declaration
5	The bidder must have its own support centers or offices in at least ten (10) locations across Tier 1 and Tier 2 cities out of which mandatorily should be in Mumbai, Hyderabad and Chennai to provide telephonic and remote assistance services. In case of exigencies or onsite support requirements at various branch locations of	Self-Declaration along with the details of the support centers and service locations across India must be submitted as part of the bid.

#	Eligibility Criteria for Bidders	Documentary Proof Required
	UIIC across India, the bidder shall arrange timely support.	
6	During the last 5 years, the bidder should have supplied, implemented, and supported the below tools for clients in PSU /Government organization /BFSI within India. • Data Loss Prevention (DLP), • Endpoint Detection and Response (EDR), • Data discovery and Data classification For each of the above tools, a minimum of two (02) references to be provided, out of which one should be of proposed OEM. The minimum deployment size required is as follows: • For Startups and MSMEs: Minimum 3000 endpoints for each tool • For rest of the bidders: Minimum 5000 endpoints for each tool	Bidder should Provide Purchase Order(s) with the performance certificate as per Annexure 18 signed & sealed by the respective Bidder's customers along with their contact details (email, mobile and landline). UIIC reserve the rights to directly interact with any of the contact submitted.
7	During the last 5 years, the proposed OEM should have been implemented for minimum two (02) clients with at least one in PSU /Government organization /BFSI within India. • Data Loss Prevention (DLP) for minimum 10000 endpoints, • Endpoint Detection and Response (EDR) for minimum 10000 endpoints, • Data discovery and Data classification for minimum 10000 endpoints,	Bidder should Provide Purchase Order(s) with the performance certificate as per Annexure 18 signed & sealed by the respective Bidder's customers along with their contact details (email, mobile and landline). UIIC reserves the right to directly interact with any of the contact submitted.

#	Eligibility Criteria for Bidders	Documentary Proof Required
	• Mobile Device Management (MDM) for minimum 2000 endpoints, • Patch Management Solution for minimum 10000 endpoints, • Key Management Solution for BitLocker key.	
8	The bidder should have deployed a minimum of at least 10 (L1 & L2) OEM certified resources/ personnels for the Proposed /Similar solutions in scope for at least one (01) PSU/ Government /BFSI client (and) Bidder should have at least 10 personnel (OEM certified) out of which 4 personnel certified for any of the proposed OEM on their direct payroll.	Details of such personnel (PO and Invoices mentioning number of resources/FMS) along with copy of OEM certificates required along with declaration stating resources are on payroll.
9	Bidder should submit the Land Border Clause as per Annexure 13.	Bidder needs to Submit Annexure 13 on letter head dully signed by Authorized signatory.

Note:

1. Bidder should submit detailed response along with documentary proof for all of the above eligibility criteria. The eligibility will be evaluated based on the bid and the supporting documents submitted. Bids not meeting the above eligibility criteria will be rejected.
2. Technical Evaluation will be done by UIIC's technical evaluation committee and the decision of the committee will be final.
3. Providing any wrong information by the bidder will result in disqualification of the bidder. The UIIC reserves the right to cross check the details submitted.
4. All Annexures must be on the letter head of the Bidder, except those which are to be provided by OEM/CA/third party/Customer. All documents' scanned copies should

be uploaded in E-NIVIDA portal and original hardcopies to be submitted to UIIC except commercial bid (refer to Tender Communication Address mentioned hereafter in this RFP for the same).

5. All documents must be signed by their authorized signatory of the respective parties and his/her designation, Official E-mail ID and Mobile no. should also be evident. Bidder has to provide the authorization letter evidencing the person signing the document is authorized to do so on behalf of his company. Inability of the bidder to prove the genuineness/authenticity of any third-party document may make the bid liable for rejection.
6. In respect of all other documents adduced by the bidder as evidence substantiating his claims, the same should be signed by the authorized signatories of the respective entities duly self-attested by the bidder authorized signatory.

2.5. Technical Scoring Criteria

#	Technical Evaluation Criteria – Parameters	Maximum Score
1	During the last 5 years bidder should have experience in supplying, implementing and supporting Mobile Device Management (MDM) for a minimum of 2000 endpoints for PSU /Government organization /BFSI client within India. • 2 References -> 0 Marks • Every additional reference -> 2 Marks subjected to maximum 4 marks (Supporting Document: Bidder should Provide Purchase Order(s) with the performance certificate as per Annexure 18 signed & sealed by the respective Bidder's customers along with their contact details (email, mobile and landline)	4
2	During the last 5 years bidder should have experience in supplying, implementing and supporting Patch Management for a minimum of 5000 endpoints for PSU /Government organization /BFSI client within India. • 2 References -> 0 Marks • Every additional reference -> 2 Marks subjected to maximum 4 marks	4

#	Technical Evaluation Criteria – Parameters	Maximum Score
	(Supporting Document: Bidder should Provide Purchase Order(s) with the performance certificate as per Annexure 18 signed & sealed by the respective Bidder's customers along with their contact details (email, mobile and landline)	
3	During the last 5 years bidder should have experience in supplying, implementing and supporting Key Management Solution for BitLocker keys for PSU /Government organization /BFSI client within India. • 1 Reference -> 0 Mark • 2 References -> 2 Marks (Supporting Document: Bidder should Provide Purchase Order(s) with the performance certificate as per Annexure 18 signed & sealed by the respective Bidder's customers along with their contact details (email, mobile and landline)	2
4	During the last 5 years the proposed OEM for Data Loss Prevention (DLP) should have been implemented for a minimum of 10000 endpoints for clients in PSU /Government organization /BFSI within India. • 2 References -> 0 Marks • Every additional reference -> 2 Marks subjected to maximum 4 marks (Supporting Document: Bidder should Provide Purchase Order(s) with the performance certificate as per Annexure 18 signed & sealed by the respective Bidder's customers along with their contact details (email, mobile and landline).	4
5	During the last 5 years the proposed OEM for Data Classification and Data Discovery should have been implemented for a minimum of 10000 endpoints for clients in PSU /Government organization /BFSI within India. • 2 References -> 0 Marks	4

#	Technical Evaluation Criteria – Parameters	Maximum Score
	• Every additional reference -> 2 Marks subjected to maximum 4 marks (Supporting Document: Bidder should Provide Purchase Order(s) with the performance certificate as per Annexure 18 signed & sealed by the respective Bidder's customers along with their contact details (email, mobile and landline).	
6	During the last 5 years the proposed OEM for Extended Detection and Response (EDR) should have been implemented for a minimum of 10000 endpoints for clients in PSU /Government organization /BFSI within India. • 2 References -> 0 Marks • Every additional reference -> 2 Marks subjected to maximum 4 marks (Supporting Document: Bidder should Provide Purchase Order(s) with the performance certificate as per Annexure 18 signed & sealed by the respective Bidder's customers along with their contact details (email, mobile and landline).	4
7	During the last 5 years the proposed OEM for Mobile Device Management (MDM) should have been implemented for a minimum of 10000 endpoints for clients in PSU /Government organization /BFSI within India. • 2 References -> 0 Marks • Every additional reference -> 2 Marks subjected to maximum 4 marks (Supporting Document: Bidder should Provide Purchase Order(s) with the performance certificate as per Annexure 18 signed & sealed by the respective Bidder's customers along with their contact details (email, mobile and landline).	4

#	Technical Evaluation Criteria – Parameters	Maximum Score
8	During the last 5 years the proposed OEM for Patch Management should have been implemented for a minimum of 10000 endpoints for clients in PSU /Government organization /BFSI within India. • 2 References -> 0 Marks • Every additional reference -> 2 Marks subjected to maximum 4 marks (Supporting Document: Bidder should Provide Purchase Order(s) with the performance certificate as per Annexure 18 signed & sealed by the respective Bidder's customers along with their contact details (email, mobile and landline).	4
9	During the last 5 years the proposed OEM for Key Management Solution for BitLocker should have been for clients in PSU /Government organization /BFSI within India. • 2 Reference -> 0 Marks • 4 References -> 4 Marks (Supporting Document: Bidder should Provide Purchase Order(s) with the performance certificate as per Annexure 18 signed & sealed by the respective Bidder's customers along with their contact details (email, mobile and landline)	4
10	Bidder should have OEM certified personnel for in-scope solutions on their direct payroll • Up to 20 certified resources -> 5 Marks • For every additional 5 certified resources -> 5 Marks subjected to maximum 20 marks (Supporting Document: Details of such personnel along with copy of OEM certificates along with declaration stating resources are on payroll)	20

#	Technical Evaluation Criteria – Parameters	Maximum Score
11	Presentation to be made by the Bidder on understanding of the requirements and proposed methodology including but not limited to: • Depth of understanding and relevance of proposed approach and methodology to the scope of work • Demonstrated experience in similar engagements with proven outcomes and domain-specific implementations • Proposed team's qualifications, certifications, and experience aligned to support the engagement requirements effectively (60 Minutes presentation which includes demonstration of solutions functionalities)	6
12	The OEM's ability to meet Technical Specification (Annexure 10). For each requirement, the OEM has to do self-assessment and update score as either 0, 1 or 2 • 0 – Feature is not feasible. • 1 – Feature is not available as part of the solution but will be provided as part of customization. OEM to provide detailed information about how the customization shall be done. • 2 – Feature is available as part of the solution Scoring out of a maximum of 40 marks can be calculated as below: Score = (Marks obtained / Total Marks) * 40 (rounded off to 3 decimal places)	40
Total		100

3. SCHEDULED EVENTS

#.	Description	
1.	Name of the Tender	SELECTION OF VENDOR FOR ONBOARDING SYSTEM INTEGRATOR (SI) TO IMPLEMENT ENDPOINT SECURITY TOOLS
2.	Tender Reference Number	000100/HO IT/RFP/282/2025-2026
3.	Tender Release Date	13-08-2025
4.	Last date for queries through Email (Tentative)	22-08-2025
5.	Pre-bid meeting (Tentative)	27-08-2025
6	EMD Fee	1,50,00,000/- (Rupees One Crore Fifty lakhs only)
6.	Last date for bid submission	08-09-2025, 12:00 PM
7.	Eligibility cum Technical bid opening	08-09-2025, 12:30 PM (Tentative)
8.	Commercial Bid opening	Will be communicated via authorized channel
9.	Address for submitting of Bids	The bidding process is completely online. Bidders are requested to submit all documents online as detailed in this RFP. For further instructions regarding submission of bids online, the bidders shall visit the E-NIVIDA portal (https://railtel.enivida.com/)
10.	Email ID for communication	rfp.infra@uiic.co.in
11.	Tender Communication Address	Deputy General Manager, Information Technology-7th floor, Head Office 24, Whites Road, Chennai – 600 014.

Note:

- UIIC reserves the exclusive right to make any amendments / changes to or cancel any of the above actions or any other action related to this RFP.
- If any of the above dates is declared a holiday for UIIC, the next working date will be considered.
- This is a non–transferable RFP document.
- A copy of Tender document is available on the web portal https://uiic.co.in/web/tenders-rfp

- Please note that the Company shall not accept any liability for non-receipt/non-delivery of bid document(s) in time.

4. SCOPE OF WORK

UIIC will award the contract to the successful bidder/s and the bidder/s should deliver the services as per the technical requirement (ANNEXURE 10) of the RFP.

Considering the enormity of the assignment, any service which forms a part of the Project Scope that is not explicitly mentioned in scope of work as excluded would form part of this RFP, and the Bidder is expected to provide the same at no additional cost to UIIC. The Bidder needs to consider and envisage all services that would be required in the Scope and ensure the same is delivered to UIIC. UIIC will not accept any plea of the Bidder at a later date for omission of services on the pretext that the same was not explicitly mentioned in the RFP.

4.1. General Requirements

- The bidder shall assess the existing endpoint and enterprise security infrastructure to identify gaps, vulnerabilities, and areas of improvement.
- Review the current IT and security infrastructure (if any), identify existing gaps, and provide recommendations for effective deployment of the proposed solutions.
- Conduct data flow mapping to identify and categorize sensitive data, and create a comprehensive inventory based on business relevance and regulatory requirements.
- Define and implement policies for data handling, access control, threat detection, device management, and compliance based on organizational needs and risk posture.
- Install, configure, and validate all required agents/components across endpoints, servers, laptops, and other applicable assets to enable full functionality of the proposed solutions.
- Enable real-time monitoring of system and user activities, generate alerts for violations or anomalies, and support incident detection, investigation, and response workflows.
- Integrate the proposed solutions with existing enterprise tools such as identity services, SIEM, endpoint management platforms, and other relevant infrastructure.

- Ensure that all deployed components comply with applicable security regulations, data protection laws, and organizational policies, and support auditability and traceability.
- Implement secure lifecycle management processes for encryption keys, access credentials, and related assets, with appropriate access controls and audit logging.
- Deliver complete technical documentation, architecture diagrams, configuration details, and conduct training sessions for administrators and relevant stakeholders.
- Provide ongoing support including incident handling, patching, upgrades, and redeployment of agents as required. Ensure the solutions are scalable and resilient to meet future needs.
- The bidder shall ensure that all the services mentioned in the scope are delivered in accordance with the technical compliance requirements outlined in the RFP ANNEXURE 10

4.1.1. Data Loss Prevention (DLP)

- The bidder shall provide an on-premises DLP solution, including all necessary underlying hardware, to ensure effective data protection across the enterprise environment.
- The bidder shall ensure compatibility with multiple operating systems, including Windows, Linux, etc. to facilitate comprehensive endpoint coverage.
- The bidder shall maintain the solution's support throughout the contract period, providing upgrades at no additional cost if the OEM declares the product end of life.
- The bidder shall implement high availability and disaster recovery functions to ensure continuous operation and data protection.
- The bidder shall provide a central console for defining policies, creating user and system groups, logging activities, deploying updates, and generating reports.
- The bidder shall ensure 24x7x365 OEM support for the DLP solution to address any operational issues promptly.
- The bidder shall implement role-based access controls (RBAC) to allow specific administrators to perform read, write, or read/write actions based on their permissions.
- The bidder shall support granular policy control based on user, device, or group, allowing for tailored data protection measures.

- The bidder shall provide remote collection capabilities for troubleshooting logs to facilitate efficient issue resolution.
- The bidder shall ensure compliance with relevant regulations.
- The bidder shall utilize modern remote deployment methods, including script support, to facilitate easy installation and uninstallation of the DLP agents.
- The bidder shall provide real-time email alerts for policy violations, ensuring timely notification of potential data breaches.
- The bidder shall generate predefined and customizable reports for audit and internal reporting purposes, with options for export in various formats (PDF, Excel, CSV).
- The bidder shall implement optical character recognition (OCR) techniques to enhance the solution's ability to detect sensitive data within images and documents.
- The bidder shall leverage AI and machine learning capabilities for anomaly detection, predictive analytics, and intelligent data discovery to enhance the effectiveness of the DLP solution.

4.1.2. Data Classification and Data Discovery

- The bidder shall deploy the data classification and discovery solution on-premises with 24x7x365 OEM support.
- The bidder shall ensure high availability of the solution at both the primary and disaster recovery sites, with seamless switching capabilities.
- The bidder shall provide scalability options to accommodate future requirements of the organization.
- The bidder shall integrate the solution with existing security technologies, including Active Directory, PAM/PIM, and SIEM systems.
- The bidder shall enable the classification of unstructured data, including Word, Excel, PDF documents, and emails from the email solution.
- The bidder shall implement metadata tagging for various file formats, ensuring proper classification and identification of sensitive data.
- The bidder shall develop user-defined classification labels, allowing users to categorize data as Public, internal, confidential, or restricted.
- The bidder shall enforce classification policies to prevent users from bypassing classification options in documents and emails.

- The bidder shall provide a centralized management console with role-based access controls for administrators and compliance teams.
- The bidder shall implement automated remediation actions for policy violations, including quarantine, deletion, and alert generation.
- The bidder shall conduct scheduled scans to automatically classify files based on properties, content, and metadata.
- The bidder shall support real-time discovery and classification of newly created or modified files through event-based monitoring.
- The bidder shall provide built-in reports and dashboards to analyze user behavior, system health, and classification activities.
- The bidder shall ensure compliance with relevant regulations.
- The bidder shall facilitate the integration of the solution with Data Loss Prevention (DLP) tools to extend enforcement based on classification results.

4.1.3. Endpoint Detection and Response (EDR)

- The bidder shall provide an EDR/XDR solution that supports Windows OS endpoints, consisting of Endpoint Protection (EPP), Anti APT, sandboxing, integrated antivirus and anti-malware, and other related EDR components.
- The bidder shall ensure that the EPP component is an on-premises solution, while the Anti APT or sandboxing solution is also hosted on-premises.
- The bidder shall implement a hybrid/on-premises EDR solution with minimal components hosted on cloud for both data center and disaster recovery. Bidder shall ensure that the cloud on which the components are hosted is located within India and no data is moved out of India as per the law of the land.
- The bidder shall ensure compatibility with multiple operating systems, including Windows, Linux, etc.
- The bidder shall maintain support for the solution throughout the contract period, providing upgrades at no additional cost if the OEM declares the product end of life.
- The bidder shall enable policy definition that includes whitelists to implement exceptions to the base policy.
- The bidder shall support high availability and disaster recovery functions to ensure continuous operation of the solution.
- The bidder shall provide a deeply functional and documented API to support integration and automation across various platforms.

- The bidder shall implement a central console for defining policies, creating user and system groups, logging activities, deploying updates, and generating reports.
- The bidder shall provide professional OEM support for 24x7x365, including on-call and remote assistance.
- The bidder shall implement role-based access controls (RBAC) to allow specific administrators to perform read, write, or read/write actions based on their permissions.
- The bidder shall allow the exclusion of files and folders from scans to enhance operational efficiency.
- The bidder shall enable the remote execution of PowerShell scripts on client machines by authorized administrators only.
- The bidder shall support the importation and prevention of custom Indicators of Compromise (IOCs) within the solution.
- The bidder shall implement secure mechanisms for registering new client installations to the solution to ensure integrity and security.

4.1.4. Mobile Device Management (MDM) for Laptops, Tablets

- The solution is expected to function like a unified endpoint management solution and shall be used for managing mobile devices such as laptops and tablets. The solution should also have the capability to manage desktops.
- The bidder shall provide a web-based MDM solution that operates over HTTPS, utilizing a single port (443) for all communications, including web services, REST APIs, and WebSocket connections.
- The bidder shall ensure that the MDM remote management software consists of a central installation only, without the need for separate site-level components.
- The bidder shall implement granular, custom-configurable admin user roles and profiles that can be mapped with Active Directory for enhanced security and management.
- The bidder shall ensure that the MDM Device Agent initiates all communications without opening local listening ports to enhance security.
- The bidder shall provide a centralized dashboard that displays hardware and software inventory, device status, health status, patch and vulnerability summaries, and alerts.
- The bidder shall support complex device configurations, including USB device security policies, application whitelisting and blacklisting, power management, and lockdown configurations.

- The bidder shall implement a Security Manager feature that allows administrators to set device lockdown and security settings, such as kiosk mode and USB security management.
- The bidder shall support location-based tracking of devices using GeoIP technology to enhance asset management and security.
- The bidder shall provide web-based remote control and shadowing capabilities for effective device management.
- The bidder shall enable incident management features, including device monitoring, preventive maintenance, and alerts for system health and performance.
- The bidder shall facilitate asset management by providing automatic inventory updates, hardware compliance checks, and software license compliance reporting.
- The bidder shall allow for the configuration of various device settings, including application restrictions, system settings, and security policies for Windows devices.
- The bidder shall provide comprehensive audit logs and reporting capabilities, including device inventory reports, location history reports, and data usage reports.
- The bidder shall support integration with existing ITSM solutions, such as JIRA and SIEM, to streamline incident management and security monitoring.

4.1.5. Key Management Solution for BitLocker keys

- The bidder should design and propose a centralized Key Management System that supports management of the BitLocker Keys.
- The bidder should ensure the KMS uses industry-standard encryption protocols and algorithms (e.g., AES-256).
- The bidder should provide a high-level architectural overview detailing key lifecycle flows and integration with other enterprise systems.
- The bidder should implement secure processes for key generation, distribution, storage, rotation, archival, recovery, and destruction.
- The bidder should support both automated and manual key rotation policies configurable by the organization.
- The bidder should ensure audit logging is enabled for all key-related activities, including generation, access, and deletion

- The bidder should enable seamless integration of the KMS with endpoint disk encryption agents installed on end-user devices.
- The bidder should provide integration support with enterprise directories such as Active Directory and endpoint management platforms.
- The bidder should ensure compatibility with SIEM tools for logging and monitoring purposes.
- The bidder should implement role-based access controls (RBAC) to govern administrative privileges within the KMS.
- The bidder should support fine-grained permission settings and approval workflows for sensitive key operations.
- The bidder should maintain logs of access attempts and configuration changes related to key management.
- The bidder should ensure the KMS is architected for high availability and includes redundancy across geographically separated locations.
- The bidder should provide disaster recovery plans and conduct regular backup and restore tests for KMS components and key material.
- The bidder should ensure that the KMS complies with applicable regulatory and industry standards.
- The bidder should protect encryption keys at rest and in transit, ensuring they are never exposed in plaintext.
- The bidder should implement real-time monitoring and alerting mechanisms for key operations and security incidents.
- The bidder should provide configurable reporting tools that generate logs and audit reports on key usage, access patterns, and anomalies.
- The bidder should deliver comprehensive documentation covering system architecture, configuration, key management procedures, and operational guidelines.
- The bidder should provide technical support during implementation, post-deployment, and for ongoing operations, including incident response and system updates.

4.1.6. Patch Management

- The bidder should assess the organization’s current patch management solution and processes, and ensure seamless alignment, integration, or augmentation without disrupting existing operations.
- Details about existing Patch Management Solution at UIIC:

No.	HCL - Client Management System Licenses			
	License Name	Product Code	Qty (Perpetual License)	Update and Upgrade support till
1	HCL BigFix Lifecycle Client Device	E0BDDLL	13000	31.03.2026
2	HCL BigFix Inventory Client Device	E0BDFLL	13000	31.03.2026

- The bidder can include the necessary update & upgrade support for the existing patch management solution or propose a different patch management solution.
- The bidder should provide a patch management solution that supports automated patch detection, approval, deployment, verification, and rollback for all supported operating systems and third-party applications.
- The bidder should ensure compatibility with the organization's current patch management tools and workflows, including support for policy-driven patch scheduling and blackout windows.
- The bidder should provide integration with Active Directory and existing endpoint management platforms to streamline patch deployment and reporting.
- The bidder should ensure the proposed solution supports remote, mobile, and offline endpoints, with capabilities for caching or peer-to-peer patch delivery to minimize bandwidth usage.
- The bidder should offer customizable patch baselines and allow exception handling for systems with non-standard requirements or patching schedules.
- The bidder should include dashboards and real-time reporting features to track patch status, compliance levels, and overall risk exposure.
- The bidder should provide audit logs and historical patch activity reports to support compliance with internal policies and external regulatory requirements.
- The bidder should implement a patch testing and staging process before full deployment to ensure stability and minimize operational disruptions.
- The bidder should ensure that all patch-related communication, data transfer, and authentication mechanisms are secure and encrypted using industry best practices.

- The bidder should ensure high availability and redundancy of the patch management system to avoid service disruption.
- The bidder should assist in defining patch deployment strategies, SLAs, and exception handling in coordination with the organization's IT and security teams.
- The bidder should conduct knowledge transfer and provide training to the organization's technical team on configuration, monitoring, troubleshooting, and reporting within the patch management solution.
- The patch management solution should have capability to extract customized report based on industry frameworks such as ISO27001.
- The bidder should ensure that the patch management solution complies with applicable security standards and guidelines.

4.2. TECHNICAL CONSIDERATIONS FOR ENDPOINT SECURITY TOOLS

4.2.1. SIZING

Solution	Type	Count
Data Loss Prevention	Endpoints & Servers	30000
	Email	
	Web	
Data Classification	Endpoint & Servers	15000
Endpoint Detection and Response	Endpoint, Servers, Mobiles (Android & iOS), Tablets (Android & iOS)	15000
Mobile Device Management	Laptops and Tablets	1500
KMS For BitLocker Keys	Endpoint	14000
Patch Management	Endpoint	20000

4.2.2. LICENSING MODEL

The licensing of the OEM should be on a perpetual model and not on a subscription model

4.2.3. SYSTEM INTEGRATOR CO-ORDINATION

Bidder is responsible for coordinating with other service providers of UIIC for any integration.

4.2.4. OEM WARRANTY AND BACK-END SUPPORT

For all the in-scope tools, the Bidder must take back-to-back OEM support for complete contract period and certificate from OEM has to be obtained for such arrangements.

During the contract period, it will be the responsibility of the Bidder to raise tickets with the OEM for the replacement of the faulty items.

4.2.5. SOLUTION ARCHITECTURE DOCUMENTATION

A detailed solution architecture, design, configuration plan, sample logs, integration with UIIC security solution (like SIEM etc.,) and other documentation as required by UIIC should be submitted. Default template of documentation should be maintained whenever a change made it has to be documented and shared to UIIC team time to time. Deployment of the solution will start only after acceptance by the UIIC.

4.2.6. DEMONSTRATION OF PROOF OF CAPABILTY

The successful bidder shall demonstrate the working of the solution with complete configuration as per UIIC requirements at one of the sites at no additional cost to UIIC. Only on successful demonstration to the satisfaction of the UIIC or any other third party appointed by UIIC, the company will issue Purchase Order. In the event of failure to demonstrate the same within a period of one month of placement of Letter of intent (LOI), the company reserve the right to cancel the tender and initiate action as per RFP.

4.2.7. BENCH MARK

On complete installation, configuration and Deployment of the solution at endpoint, the bidder shall demonstrate the scalability of a solution with 10,000 endpoints using automated simulations and outcome of such report shall be submitted to UIIC. In the event the solution does not scale up to the above load, the bidder at his cost shall replace/augment the infrastructure.

4.2.8. TRAINING

- The bidder shall arrange the training program from OEM for at least three officials of UIIC preferably at the OEMs training centers at no cost to UIIC.
- Training material for the program shall be provided by the bidder both as hard and soft copy.

- The training should cover all aspects of the solution which includes system administration and policy management, report generation and other relevant features of the solution.

4.2.9. END OF SALE AND END OF SUPPORT

The solution proposed by the bidder should not reach End of Life (EOL) or End of Support (EOS) during the entire duration of the contract. In the event either EOL or EOS or both are declared the bidder shall replace such solution components at no cost to UIIC immediately. The bidder must provide details of the EOL and EOS certification from the OEM and OEM data sheet.

4.2.10. MANUALS/DOCUMENTATION

Soft and hard copies of User and Technical manuals are to be provided for all the functionalities /modules/hardware/tools proposed for the solution separately. The bidder shall also ensure updated manuals are available in the OEM website

4.2.11. KNOWLEDGE TRANSFER

At the end of the contract period the bidder shall complete knowledge transfer to any new vendor on boarded by UIIC.

4.2.12. OPEN-SOURCE SOFTWARE

All Open-source tools / software / hardware / utilities / as a part of the solutions shall come with enterprise support in India.

5. PROJECT TIMELINE

- The bidder has to adhere to the timelines specified in the below table. The timelines specified for each month in the below table are from the date of issuance of Purchase Order. The bidder is expected to factor in all effort required to adhere to these timelines. The UIIC will not accept any plea by the bidder later date for deviating from these timelines on the pretext that the same was not explicitly mentioned in the RFP.
- The bidder has to submit a detailed plan for migration and implementation of the solution. Plan should include the full scope of the project as mentioned above. On acceptance of such plan by UIIC, the bidder is required to carry out the implementation, and customization as applicable including supply, installation, and testing of solution etc. The bidder shall also handle all matters relating to the configuration and operation of the system including but not limited to application,

system interfaces, documentations, User manual and training for the successful implementation of the system.

5.1. TIMELINE

#	Activity	Timeline
1	Issuance of Purchase order	--
2	Design of the solution architecture, pre-requisites gathering, and initial assessments as necessary	Within 2 weeks from the date of Purchase Order issuance
3a	Delivery of hardware and software components at Mumbai & Hyderabad locations	Within 6 weeks from the date of Purchase Order issuance
3b	Deployment of agents of in-scope tools on all endpoints across all locations of UIIC	In parallel with hardware delivery; Within 6 weeks from Purchase Order
4	Infrastructure setup and base configuration (racking, cabling, OS, and solution installation)	Within 10 weeks from the date of Purchase Order
5	Integration of deployed agents with backend systems and activation of policies	Within 12 weeks from the date of Purchase Order
6	Final solution configuration and user acceptance	Within 14 weeks from the date of Purchase Order
7	Go-live across all locations	Within 14 weeks from the date of Purchase Order
8	Post-deployment activities including preparation of SOP and hardening document, training and knowledge transfer sessions	Within 16 weeks from the date of Purchase Order

The entire project needs to be completed expeditiously. The UIIC and the selected Bidder shall nominate a Project Manager immediately on acceptance of the order, who shall be the single point of contact for the project at Chennai. However, for escalation purpose, details of other people shall also be given. The project manager nominated by the Bidder should have prior experience in implementing similar projects. Project kick-off meeting should happen within 7 days from the date of Letter of Intent (LOI).

6. INSTALLATION AND CONFIGURATION

- Bidder should install all ordered equipment's supplied for the smooth functioning of the Endpoint Security solutions.
- UIIC reserves the right to involve experts and independent consultants to validate the implementation, as necessary.

- All the installation and configuration shall be under the direction and guidance of the OEM.
- Bidder shall be responsible to generate detailed documentation for the entire installation/configuration, troubleshooting procedures, etc.
- Detailed architecture of the solution should be handed over to the UIIC both prior and post the implementation stage (including the modifications made in the architecture if any, during the implementation stage).
- The implementation will be deemed complete when all the supplied devices including hardware, operating systems, licenses, database, supporting software, drivers, etc. are installed and accepted by the UIIC. The new Endpoint Security Solution should be configured with all the policies and moved to the production environment.

7. SUPPORT ENGINEERS

Bidder shall deploy qualified resources with valid certification and relevant experience for conducting the in-scope activities at UIIC Premises.

#	Responsibilities	Experience	Count
1	Project Coordinator: • Develop a comprehensive project plan, including objectives, timelines, and resource requirements. • Establish effective communication channels and maintain positive relationships with stakeholders. • Identify and mitigate project risks, both technical and non-technical. • Maintain accurate project documentation, including technical specifications. • Ensure project deliverables meet established quality standards.	15 Years of experience: Documentary proof for the same should be submitted.	1

#	Responsibilities	Experience	Count
	• Should share the contact details for communication purpose.		
2	L2 Resource: • Detailed plan for deployment Source. • Liaise with the end users, in consultation with the UIIC, for resolution of end users problems • One dedicated LEVEL 2 engineer at onsite (Head Office-Chennai) • Submission of the revised documentation whenever major changes are performed which should include the revised architecture and logical setup diagram. • Should be SPOC for UIIC officials and immediate responsible for all the configurations, policies and changes required by UIIC as and when required	L2 Resource- Minimum 5 years of experience in the proposed Endpoint Security solutions. Should have OEM level or its equivalent level Certification at Endpoint Security solution. Note: Copy of Experience certificate and performance certificate (If any) shall be submitted to UIIC and the same shall be verified by UIIC in addition to the bidder evaluation. In case of any deviation, It's bidders responsible to replace the L2 resource with no additional cost.	L2 Resource – 6 (one per solution) (General shift 9.30 AM to 7.00 PM) at UIIC Head Office, Chennai. Working days = As per UIIC working days and will be available for support whenever required by UIIC
3	L1 Resource: • Detailed plan for deployment Source. • Liaise with the end users, in consultation with the UIIC, for resolution of end users problems • One dedicated LEVEL 1 engineer at onsite (Head Office-Chennai) • Submission of the revised documentation whenever major changes are performed which should include the revised	L1 Resource- Minimum 2 years of experience in the proposed Endpoint Security solution. Should have OEM level or its equivalent level Certification. Note: Copy of Experience certificate and performance certificate (If any) shall be submitted to UIIC and the same shall be verified by UIIC in addition to the bidder evaluation. In case of any deviation, It's bidders responsible to replace	L1 Resource – Per Shift one resource in HO, one in DC and one in DR (24x7)

#	Responsibilities	Experience	Count
	architecture and logical setup diagram. • Should be SPOC for UIIC officials in case of L2 resource not available and immediate responsible for all the configurations, policies and changes required by UIIC as and when required	the L1 resource with no additional cost.	

- **TERMS AND CONDITIONS**:
  - Resource should be available at any time in case of scheduled as well as ad hoc activity to provide seamless support.
  - Onsite or OEM-level support must be provided for all endpoint security issues that cannot be resolved by L1 or L2 support engineers.
  - Bidder should come up with software or tool with no additional cost to record deployed resources attendance (will be shared to UIIC on weekly basis) to verify the same with UIIC's attendance register for the payment purpose.

- **SCOPE OF ONSITE RESOURCES INCLUDES**:
  - Managing the in-scope solution at Data Center & Disaster Recovery Site. In case of exigency, resource should be available at both the sites. However, the associated costs will only be incurred and considered at the time of actual utilization.
  - Shall provide an escalation matrix in consultation with the IT Department, Head Office, UIIC for different categories of support calls.
  - Day-to-day maintenance performed to the solution setup which may be provided by UIIC.
  - Should be conversant with the regular Configuration from scratch, administration tasks, patch management, user management, backup procedures etc.
  - Should be able to troubleshoot problems raised and should maintain a log of them, also report it to the UIIC officials in detail with root cause analysis and problem resolution.

- The Bidder should ensure that there will be a proper change & configuration management, backup management, security management. These procedures should be well documented, followed and maintained (copy of the same should be submitted to UIIC)
- The onsite support Personnel should be capable of re-install/ reconfigure any component/ system of the security equipment supplied by the vendor, in case of crash of those components /system on problem or patch/upgrades. The on-site Support Personnel also needs to support, if any security installations done by a separate vendor.
- In case the problem is not being rectified by the onsite L1 & L2 Personnel even after 1 hour, the issue should be escalated and resolved within 5Hrs from time of incident.
- The support Personnel should also keep track of the issues /ticket raised through the web interface help desk/telephone/mail etc. and should provide the solution for the same.
- Upgradation of products to the latest version, whenever applicable. The procedures have to be documented and submitted to UIIC before carrying out any such activity.
- The vendor has to do necessary implementations required from business continuity perspectives.
- Make addition/changes/deletion of rule/policy etc. as per UIIC's requirement.
- Applying update, upgrade, patches, fixes etc.
- Backup of log, configuration, data etc.
- Report preparation, generation etc.
- Documentation and architectural/logical diagram reviewing, revising and submitting on regular basis (as and when required)
- Monitoring the HW, SW and Applications' health and utilization.
- Call log, Follow-up, escalation for resolving issues
- Generate alert for UIIC team through multiple medium.
- Scheduling automatic backup to the storage devices on regular basis and retrieving old backups as and when required.
- Co-ordination with UIIC team for ensuring smooth operation of the solution.
- Knowledge transfer to UIIC employees (as and when required).
- Maintain downtime register

8. SERVICE LEVEL AGREEMENT AND PENALTIES/LIQUIDATED DAMAGES:

8.1. EQUIPMENTS SUPPLIED BY BIDDER

The selected Bidder shall guarantee a quarterly uptime of **99.9%** for the entire Solution from the date of commissioning/Go-Live during the warranty and AMC period. (Any planned shutdown will not be considered for calculating SLA).

The percentage of **uptime** is calculated on quarterly basis as follows:

$$\frac{\text{(Total contracted minutes in a quarter – downtime during contracted minutes) *100}}{\text{Total contracted minutes in a quarter.}}$$

*Example: If there are 92 days in a quarter, then total time would be 1,32,480 minutes. The acceptable downtime would be 132 minutes for making full payment for the quarter based on the following calculations: - (132480 -132)/ 132480*100 = 99.90%*

The table below specifies support/maintenance matrix along with mean time to respond (MTTR1) and mean time to resolve (MTTR2).

SN.	OFFICE	MTTR1	MTTR2
1.	DC- Mumbai	00:15	04:00
2.	DR- Hyderabad	00:15	04:00

Response Time: - Defined as time taken by the help desk of the bidder to respond to the concerned user over the service desk tool/phone/Email or in person and acknowledge the problem. Same is applicable when there is a problem with the proposed solution.

Resolution Time: - Defined as time taken to resolve a problem, which includes RMA (Return Merchandise Authorization) in case of entire Hardware failure at any one of the sites.

The above maintenance timelines are applicable for all the three years of warranty period and further two years of AMC period, for all equipment and related components being supplied by the Vendor as per the scope of this RFP.

The equipment SLA is invoked whenever any equipment/module is not functioning as planned (not necessary for the end users to face downtime arising out of this). The malfunction can be caused due to any reasons including hardware error, misconfigured device settings, incompatible OS patch, wrong OS upgrade etc. Non-functioning of any module in the equipment would also lead to penalty as specified. For example, it will invoke SLA but when there is a planned downtime during weekend for non-business days for system upgrades etc. it will not invoke SLA provided permission for downtime is obtained in writing at least one day prior to such activity.

Further, all Critical, High, Medium and Low priority incidents should be logged as incident tickets. Incidents details along with action plan/ mitigation steps should be alerted to UIIC personnel and resolved as per the below SLA:

Severity Level	Resolution Time	Penalty
Critical (P1)	2 Hours	₹1,000 per incident exceeding SLA by one hour will be recovered from the bidder
High (P2)	4 Hours	
Medium (P3)	6 Hours	
Low (P4)	8 Hours	

8.2. MAINTENANCE PENALTY FOR THE EQUIPMENTS SUPPLIED BY BIDDER

Uptime (U)	Penalty
U >=99.90	No Penalty
Uptime < 99.90	0.01 % of Solution cost for every 1 hour or part thereof in excess of U >=99.90 subject to Maximum of 10% of Solution cost. Beyond which UIIC may terminate the contract.

Appliance uptime should be provided in interface/console/CLI and services uptime should be provided using SNMP configuration as a proof further it will be verified by UIIC officials on time of submission of invoices for the quarterly payment of services. SLA should be calculated based on both appliance and service uptime. If solution

components at any one of the sites is down exceeding MTTR2 time limit, then also penalty will be applicable.

The problem shall be considered to be solved under following conditions:

1 The vendor has replaced the faulty part / entire equipment and configured it to function normally.
2 The vendor has given a working substitute for the faulty equipment.

The problem shall be considered to be unsolved under following conditions:

1 The vendor has neither responded nor replaced the faulty part / equipment
2 The vendor has responded but not replaced the faulty part / equipment
3 The vendor has responded and replaced the faulty part / equipment but the problem is not solved.
4 The vendor has responded and replaced the faulty part / equipment but did not configure it properly to work in the desired fashion.

The down time will be calculated on quarterly basis. The downtime calculated shall not include the following:

1 Downtime due to hardware/software and application which is owned by UIIC and at the instance of UIIC.
2 Negligence or other conduct of UIIC or its agents, including a failure or malfunction resulting from applications or services provided by UIIC or its vendors
3 Failure or malfunction of any equipment or services not provided by the bidder.
4 However, it is the responsibility/ onus of the selected bidder to prove that the outage is attributable to UIIC. The selected bidder shall obtain proof authenticated by UIIC's official that the outage is attributable to UIIC.

Record of call resolution is to be jointly signed by the bidder/System integrator and UIIC personnel marking nature of fault attended and steps / initiatives taken to resolve the service call of the company.

- SLA will be monitored on quarterly basis.
- Penalty due to downtime, during contract period will be deducted from any subsequent payment to be made to the Successful bidder.
- Penalty due to downtime, during AMC/ATS period will be deducted from AMC/ATS payment.

8.3. RESOURCES PROVIDED BY BIDDER AND PENALTY

The resident engineers stationed at UIIC's HO will be exclusively for this project and cannot be shared by the bidder for any other purpose during contract period. Granting leave/ absence to the engineers posted at our site, should be with at least 2 days' prior intimation to the UIIC and suitable replacement should be arranged in his/her absence without fail. Penalty may attract if engineers are absent.

1. During the Implementation period - In the absence of the engineers (both L1 & L2 engineer), suitable replacement is to be provided on immediate basis. In case of absolute absence (when no replacement is provided), penalty would be deducted @2 Man days cost (either L1 or L2 depends on the absent resource) for each day.
2. During the Contract Period - In the absence of the engineer (both L1 & L2 engineer), suitable replacement is to be provided on immediate basis. In case of absolute absence (when no replacement is provided), penalty would be deducted @1.5 Man Day cost (either L1 or L2 depends on the absent resource) for each day.
3. Engineer Support @ DC and DR – In case of exigency or in case of engineer requirement at DC and DR sites, Bidder should provide support at the DC and DR within 3 hours from the time of incident reported, if not penalty would be deducted @ 1 Man Day cost (L2 Man days cost) for each hour of delay.

8.4. PENALTY DUE TO ERRONEOUS BEHAVIOR OF THE SOLUTION

If the solution, or any of its components behaves erroneously which results in monetary or business loss to the UIIC, then the entire amount of such loss shall be recovered from the bidder on actual basis.

Maximum deducted penalty of one type will not affect any other type of penalty i.e. all the types of penalties can be levied up to their maximum limit simultaneously and shall not exceed 10% of the total contract value.

UIIC reserves the right to Cancel the Purchase Order, Terminate the Contract, Forfeit the Performance Bank Guarantee and Blacklist the Successful bidder, in case the Successful bidder exceeds the threshold limit of Delay for any of the items above. UIIC, at its sole discretion, may exercise any or all of the options against the Successful bidder, in such circumstances.

9. RESPONSE WARRANTY & AMC

- The bidder as part of this RFP should provide a 24/7 response in case of appliance failure during operations. Additionally, the OEM of the Endpoint Security tools must ensure that all the component spares are readily available from their respective offices in Mumbai (Data Center) and Hyderabad (Disaster Recovery site).
- The bidder must provide comprehensive onsite warranty of 3 years and AMC support of 2 years for all the hardware/software component of the proposed solution.
- Annual Maintenance Contract:
    - Support for maintenance of Hardware items supplied should be available for a minimum period of 2 years, covering all parts, maintenance and support, after expiry of warranty period of 3 years.
    - The UIIC will pay AMC charges for appliance after the end of warranty period. Such payment shall be released quarterly in arrears after satisfactory completion of service during the period and submission of reports and invoices. All applicable Taxes will be paid at actual
    - During the Warranty and AMC period, the Bidder should extend the On Site Service Support. The scope of Warranty and AMC shall include:-
    - Rectification of Bugs/defects if any.
    - Preventive Maintenance quarterly.
    - Ensure Uptime of as per SLA
    - Maintenance of Servers and Other Items
    - Installation / re-installation / maintenance / reconfiguration System software and other supplied software
    - All system patches, upgrade, service packs etc. of the OS and all other software supplied must be made available free of cost.
    - Support for integration and update of infrastructure / network configuration and change management of the entire solution (existing as well as that procured as scope of this tender) to meet business requirements.
    - Provide on-site comprehensive support for the supplied items – equipment / systems / subsystems (hardware / software). Such support should include replacement of defective parts / equipment and / or repair of the same and must be considered within the scope of the project.

- In the event bidder fails in their obligations to provide the product upgrades (including management software upgrades and new product feature releases) within 30 days of release / announcement, the OEM should assume complete responsibility on behalf of the bidder to provide the same to the UIIC at no additional cost to the UIIC and install the same at the UIICs premises.

9.1. MEAN TIME BETWEEN FAILURE (MTBF)

If during the warranty period and AMC period, any hardware items fails/impaired on three or more occasions in a quarter, such hardware items shall be replaced by equivalent/superior hardware items by the bidder at no additional cost to the UIIC.

10. PAYMENT TERMS AND PENALTY DUE TO DELAY:

Item	Expected Timeline	Payable on Delivery	Payable on Go-Live	Other Payables	Penalty	Max Penalty
Delivery of Hardware	Within 6 weeks from the date of Purchase Order	60% of hardware cost	40% of hardware cost	N/A	0.5% of the payable amount for each week of delay	10% of payable amount
Delivery of Software Licenses & Agent Installation	Within 6 weeks from the date of Purchase Order	60% of software cost	40% of software cost	N/A	0.5% of the payable amount for each week of delay	10% of payable amount
Implementation (Infra setup, integration, configuration)	Within 14 weeks from the date of Purchase Order	0%	80% of implementation cost	N/A	0.5% of the implementation cost for each week of delay beyond 14 weeks	10% of implementation cost
Documentation, SOP, Training, Knowledge Transfer	Within 16 weeks from the date of Purchase Order	0%	20% of implementation cost	N/A	0.5% of the implementation cost for each week of delay beyond 16 weeks	10% of implementation cost

Item	Expected Timeline	Payable on Delivery	Payable on Go-Live	Other Payables	Penalty	Max Penalty
Facility Management Services (FMS) – L2 Resource	To commence from the date of installation of components	0%	0%	Payable quarterly in arrears	0.5% of FMS resource cost per week of absence or delay	10% of total quarterly FMS value
Facility Management Services (FMS) – L1 Resource	To commence within one week of issuance of Purchase order	0%	0%	Payable quarterly in arrears	0.5% of FMS resource cost per week of absence or delay	10% of total quarterly FMS value
AMC (Updates & Upgrades)	Commences from the date of go-live	0%	0%	Payable quarterly in arrears	0.5% of AMC value per week of delay in commence ment	10% of AMC value

NOTE: For the purpose of this clause, part of the week is considered as a full week.

10.1. CALL LOGGING

- The bidder should have a 24*7 support center during all 365 days of the year in order to log tickets.
- The support center telephone numbers should be provided to the UIIC. During the contract period, it is the responsibility of the bidder to raise complaints/tickets with the OEM for replacement of the faulty item.

10.2. LOCATION ADDRESS

DC, Mumbai	Airoli, Navi Mumbai, Maharashtra - 400 708
DR, Hyderabad	Madhapur, Hitech City, Hyderabad, Telagana – 500 004.
NDR, Mumbai	Andheri, Maharashtra.
UIIC-HEAD OFFICE	Whites Road, Chennai – 600 014.

Note: Bidder shall ensure the agents of the in-scope security solutions are deployed across all locations of UIIC as mentioned in its website.

11. EVALUATION METHODOLOGY FOR ELIGIBLE BIDDER

Technical Evaluation of the bidders who qualified eligibility criteria will be carried out based on Minimum functional & Technical specifications (ANNEXURE 10). Bidders shall submit proof of document for criteria detailed above along with the technical bid. It shall be the responsibility of the bidders to submit relevant proof of document. The bidders who are technically qualified will be considered for commercial opening.

11.1. PROCEDURE FOR SUBMISSION OF BIDS

Tender Bidding Methodology: 'Single Stage Online submission & Two stage online opening' [Eligibility cum Technical Bid & Commercial Bid]. The bidding process is completely online.

Bidders are requested to submit all seal & signed scanned documents online as detailed in this RFP. In addition to scanned documents, bidders should submit original hard copy of EMD (Annexure 5) and NDA (Annexure 9) to UIIC Head Office at Chennai at least two days before tender submission date. Any other documents may be submitted in original hard copy, if demanded or a clarification is sought in this regard.

11.2. EARNEST MONEY DEPOSIT

The intending bidders shall submit Bank Guarantee (REF. Annexure 5: Bank Guarantee Format for EMD)/Electronic Credit for EMD of Rs. 1,50,00,000/- (Rupees One Crore Fifty lakhs only). Bid will be treated as non-responsive and will be rejected in the absence of any one of the above mentioned. Bank Guarantee shall be drawn in favor of "United India Insurance Company Limited" payable at Chennai. The Bank Guarantee submitted as EMD should have a validity of 6 months.

In case of Electronic Credit, the E.M.D shall be credited to our Bank Account as given below:

Beneficiary Name	United India Insurance Company Ltd.
IFSC Code	INDB0000007

Account No.	200999095210
Bank details	IndusInd Bank
Remarks	RFP 282

The EMD will not carry any interest. The electronic credit should be affected positively at least two days prior to the tender submission date.

11.3. Forfeiture of E.M.D

The EMD made by the bidder will be forfeited if:

- The bidder withdraws the tender after acceptance.
- The bidder withdraws the tender before the expiry of the validity period of the tender.
- The bidder violates any of the provisions of the terms and conditions of this tender specification.
- The successful bidder fails to furnish the required Performance Security within 15 days from the date of receipt of LOI (Letter of Intent)

11.4. Refund of E.M.D

EMD will be refunded to the successful Bidder on production of a performance guarantee and signing of contract as per timelines defined in the RFP.

In case of unsuccessful bidders, the EMD will be refunded to them at the earliest after expiry of the final bid validity and latest on or before the 30th day after the award of the contract.

11.5. Exemption from payment of EMD (Earnest Money Deposit).

Note: Micro and Small Enterprises (MSEs) as defined in MSE Procurement Policy issued by Department of Micro, Small and Medium Enterprises (MSME) assigned with Enterprise items selling and startups recognized by Department for Promotion of Industry and Internal Trade (DPIIT) are exempt from submission of EMD (Bid Security). Bidders claiming exemption of EMD under this rule (170 of GFR) are however required

to submit a signed Bid Securing Declaration accepting that if they withdraw or modify their Bids during the period of validity, or if they are awarded the contract and they fail to sign the contract, or to submit a performance security before the deadline defined in the request for bids document, they will be suspended for the period of 12 months from being eligible to submit bids. Non submission against the same at Pre-qualification stage, will disqualify the bidder.

11.6. Instructions to Bidders for Online Submission

- The bidders can access the documents in the E-NIVIDA portal https://railtel.enivida.com/
- The relevant tender documents can be downloaded from the e-tendering site or from https://uiic.co.in/web/tenders-rfp
- The bidders should mandatorily fill in all relevant details as per the requested format in the e-tendering portal.
- The bidders are required to submit scanned documents of their bid electronically on the E-NIVIDA Portal using valid Digital Signature Certificates.

11.7. Late Bids

Bidders are advised in their own interest to ensure that bid is submitted well before the closing date and time of the bid. Any bid received after the deadline for submission of the bid, will be rejected.

11.8. Bid Preparation

- Bidder should take into account any corrigendum published on the tender document before submitting their bids.
- Please go through the tender advertisement and the tender document carefully to understand the documents required to be submitted as part of the bid.
- Any deviations from these may lead to rejection of the bid.
- Bidder, in advance, should get ready the bid documents to be submitted as indicated in the tender document/schedule and generally, they can be in PDF/XLSX etc. formats.
- Bidder to log into the site well in advance for bid submission so that he/she uploads the bid in time i.e. on or before the bid submission time. Bidder will be responsible for any delay due to any other issues.

- The bidder to digitally sign and upload the required bid documents one by one as indicated in the tender document.
- Bidders to note that they should necessarily submit their financial bids in the prescribed format given by Company and no other format is acceptable.
- Bid once submitted on E-NIVIDA shall be treated as final and no further amended bid will be accepted. However, if UIIC amends the RFP before expiry date of bid submission and a bidder had already submitted his bid, the competent authority at its discretion shall permit fresh submission of bids before the expiry date of bid submission.
- Any offline bid/tender shall not be accepted and no request in this regard will be entertained whatsoever.

11.9. Opening of Bid By UIIC

- Bids will be opened on E-NIVIDA portal as per the guidelines/Procedure at the date & time mentioned in the RFP.
- UIIC however reserves the right to extend the last date for submission of bids without assigning any reasons and such extensions shall be published on UIIC's website (https://uiic.co.in/web/tenders-rfp) as well as in E-NIVIDA portal.

11.10. Pre-Bid Meeting

- Pre-bid meeting would be held as per the date specified in the Bid Schedule.
- Only authorized representative of Bidders (not exceeding two) would be allowed to participate in the Pre-bid meeting.
- Pre-bid queries should be mailed to us in the email < rfp.infra@uiic.co.in> in the attached format as per **Annexure 14**.
- Queries received after the due date as mentioned in Bid Schedule will not be entertained.
- Replies to the Pre-bid queries would be published on UIIC's website (https://uiic.co.in/web/tenders-rfp) as well as in E-NIVIDA portal.
- Pre-bid Queries, if any, may be communicated through an email to aforementioned email id. The subject of the mail should be "Queries for Implementing Endpoint Security Tools". No other form of communication will be entertained. All queries must be sent to the email ID specified by the date as mentioned in this document.

- UIIC shall provide the clarifications to the queries raised by participant(s) in the pre-bid meeting. The pre-bid meeting will be held at below address or through video conference (Online), UIIC will inform the same.

  7th Floor, United India Bhavan,
  United India Insurance Co. Ltd.
  Head Office, 24, Whites Road
  Chennai – 600014

- It is necessary to inform UIIC well in advance, the name(s) of the representative(s) of Participant(s), who will be attending the session as scheduled above, along with an authorization letter signed by the Competent Authority of participant(s). This can be communicated through an email on < >
- Participation in the Pre-Bid meeting is non-mandatory. However, it is advisable that participant(s) attend this meeting which would be mutually beneficial.

11.11. Evaluation of Bids

UIIC will scrutinize the Bids received to determine whether they are complete in all respect as per the requirement of RFP, whether the documents have been properly signed and whether items are offered as per RFP requirement, whether documentation as required has been submitted. UIIC may, at its discretion, waive any minor nonconformity or any minor irregularity in the bid which does not constitute a material deviation. UIIC decision with regard to 'minor non-conformity' is final and the waiver shall be binding on all the bidders and UIIC reserve the right for such waivers.

11.12. Procedure for Processing the Bid Document

- The bids would be opened by the Committee constituted by the Company.
- Failure to submit any documents under any of the sections could lead to rejection of bids.
- The Committee will open the Eligibility cum Technical bids of those bidders who have submitted all the necessary documents as applicable.
- The Committee will open the Commercial bids of those bidders who qualify the minimum eligibility and technical requirements. The date & time of opening the Commercial Bids would be intimated to the qualified bidders.
- The Committee will declare successful bidder after final evaluation of bids and the result will be published on UIIC's website (https://uiic.co.in/web/tenders-rfp) as well as in E-NIVIDA portal.

- This procedure is subject to changes, if needed and the procedure adopted by the Company for opening the tender shall be final and binding on all the parties.

12. Selection Process

Participants should satisfy the basic eligibility criteria (**ANNEXURE 6**). Based on the bid submitted, Technical Bid Evaluation would be done as per Annexure 7, to short list eligible participant(s). Only those participant(s) who qualify in the Technical Bid Evaluation will be considered for Commercial Evaluation. UIIC has opted for Quality and Cost Based System (QCBS – Offline Mode in E-NIVIDA Portal) method for this RFP for evaluating the tenders.

a) The bidder who successfully qualifies in the eligibility criteria (Annexure – 6), only their technical bids will be subsequently opened for further evaluation.

b) The minimum score for successful qualification of the bidder in the Technical Scoring (Annexure – 7) will be 70% (seventy percent).

c) The bidders who qualify the technical evaluation will have to provide a Technical Presentation on the in-scope services to UIIC. The schedule and venue of the same will be conveyed accordingly.

d) If any deviations are observed during technical evaluation, UIIC may decide to accept them at its discretion, which will apply to all bidders, before opening of the Commercial Bids and the decision of UIIC in this matter will be final.

e) The technically qualified bidders will be intimated by email/letter about the date and time of opening of their 'Commercial Bid (indicative price)'. The technical scores of the bidder will be disclosed to each individual bidder on the date of opening of the commercial bid).

f) No price variation/adjustment or any other escalation will be entertained after the closing of Bids

g) However, the UIIC may, at its discretion, reduce the validity period of the tender.

h) Computation Methodology for rating bidders on 'Technical plus Commercial basis':

i) There would be a weightage of 70% to the technical score and 30% for the final Commercial price quoted by the bidder at the end of online reverse auction.

j) It would be normalized as under for each bidder: -
Total Score (up to 3 decimals) = $\{(T \times 0.7) / T_{high}\} + \{(L_{Low} \times 0.3) / L\}$, Where

- T - stands for bidder's technical evaluation score
- T_{high} - stands for the score of the technically highest Bidder
- L - stands for bidder's final commercial quote at the end of online reverse auction,
- L_{Low} - stands for the lowest final commercial quote among all bidders at the end of online reverse auction

k) The proposals will be ranked in terms of Total Scores arrived at as above. The proposal with the highest Total Score will be considered first for award of contract and will be invited for price negotiation, if required. Example:

SN	Name of the Bidder	Technical Evaluation Marks (T)	Final Commercial Bid Price (L)	$(T / T_{high}) * 0.70$	$(L_{Low} / L) * 0.30$	Total Score (S)	Rank for techno-commercial
1.	ABC	90	80	(90/90) *0.7 = 0.7	(70/80) *0.30 = 0.263	0.963	**1**
2.	DEF	85	75	(85/90) *0.7 = 0.661	(70/75) *0.30 = 0.280	0.941	**2**
3.	GHI	80	70	(80/90) *0.7 = 0.622	(70/70) *0.30 = 0.3	0.922	**3**

l) In the above example, ABC, with the highest total score of 0.963 becomes the successful Bidder.

m) In the case of tie between two or more Bidders, a bidder with highest score in technical evaluation will be declared as successful bidder.

n) In case, the successful bidder (e.g. ABC) fails to fulfil any of the obligations under the RFP within the timelines defined, UIIC reserves the right to cancel his/her selection and declare the bidder with rank 2 (DEF) as successful bidder and so on and so forth.

o) The Letter of Intent along with Purchase Order will be issued to the successful bidder. The required PBG should be submitted to UIIC within 28 days from the date of letter issued by UIIC for selection as the "selected vendor".

12.1. The Company Reserves the Right To

- Accept / Reject any of the Tenders.
- Revise the quantities at the time of placing the order.

- Add, Modify, Relax or waive any of the conditions stipulated in the tender specification wherever deemed necessary.
- Reject any or all the tenders without assigning any reason thereof.
- Award contracts to one or more bidders for the item/s covered by this tender.
- Seek clarifications from the prospective bidders for the purpose of finalizing the tender.

12.2. Rejection of Tenders

The tender is liable to be rejected inter-alia:

- If it is not in conformity with the instructions mentioned herein,
- If it is not accompanied by the requisite proof of tender document fee paid.
- If it is not accompanied by the requisite Earnest Money Deposit (EMD).
- If it is not properly signed by the bidder.
- If it is received after the expiry of the due date and time.
- If it is evasive or incomplete including non-furnishing the required documents.
- If it is quoted for period less than the validity of tender.
- If it is received from any blacklisted bidder or whose past experience is not satisfactory.

12.3. Validity of Tenders

Tenders should be valid for acceptance for a period of at least 180 (Hundred and Eighty days) days from the last date of tender submission. Offers with lesser validity period would be rejected.

12.4. General Terms

- The successful bidder shall sign the agreement within 7 days from the date of Letter of Intent (LOI) from UIIC.
- The agreement shall be in force for a period of 5 (FIVE) years & 6 months from the date of issue of Purchase Order and may be extended on mutually agreed terms.
- The offer containing erasures or alterations will not be considered. There shall be no hand written material, corrections or alterations in the offer.
- Addendum/Amendments/Corrigendum, if any, will be communicated through UIIC e-Tendering portal (https://railtel.enivida.com/) only. UIIC reserves the right to cancel the tender at any time without incurring any penalty or financial obligation to any bidder.

- UIIC reserves its right to carry out inspection of the proposed solution facility, if required. There shall not be any additional charges for such inspection.
- UIIC is governed by provisions of the Public Procurement Policy for Micro and Small Enterprises (MSEs) as circulated by The Ministry of MSME, GoI. The policy details are available on the website www.dcmsme.gov.in
- These provisions shall be applicable to Micro and Small Enterprises (MSEs) registered with District Industries Centres or Khadi and Village Industries Commission or Khadi and Village Industries Board or Coir Board or National Small Industries Corporation or Directorate of Handicrafts and Handloom or any other body specified by Ministry of Micro, Small and Medium Enterprises (MSMEs).
- Such MSEs would be entitled for exemption from furnishing tender fee and earnest money deposit (EMD) if any. In case of any issue on the subject matter, the MSE's may approach the tender inviting authority to resolve their grievances.
- Agencies/ Bidders desirous of availing exemptions/ preference under above provisions should submit a copy of proof of Registration as MSEs, and ownership of the same by SC/ST if applicable along with the tender/RFP

12.5. Security Deposit

The successful bidder will have to furnish a security deposit to the tune of 5% of the total contract value in the form of a Bank Guarantee for a period of 5 years & 3 months obtained from a nationalized/scheduled bank for proper fulfilment of the contract.

13. GENERAL TERMS & CONDITIONS OF CONTRACT

13.1. Contract Terms for Service Provider and Exit

- Contract Period: The contract will be valid for a period of 5 years from the date of issuance of purchase order. Irrespective of the period, the contract will deem to be operative until close of assigned projects as per agreed Scope of Work, and hence bidders deploying resources should ensure the resources availability until completion of the work in hand or till the extended period as per the project terms and conditions.
- Price discovered during the RFP will be valid till the completion of the project or the extended completion period as required by UIIC in respect of that project.
- UIIC reserves the right to terminate the contract at any time without assigning any reasons thereof. However, there are specific termination clauses which must be adhered by the selected vendor for continuation of contract.
- The charges proposed by short listed participants and agreed to by UIIC for the activities covered under scope of RFP shall remain frozen during the term of contract, i.e., for a period of 5 years.
- The Agreement and Service Level Agreement shall be as per the SLA clause.

- The detailed terms and conditions governing the contract shall be included in the Agreement and Service Level Agreement and may undergo changes as per the Outsourcing guidelines and/or any other Guidelines issued by IRDAI from time to time or any regulation issued by Government of India or its statutory bodies. There shall be penalties applicable on non-adherence to service deliverables as per penalty clauses.
- The selected vendor should provide satisfactory indemnities to UIIC against possible financial and / or reputational loss arising as per the indemnity clause.
- The performance of selected vendor shall be reviewed periodically, for continuation of the contract. Any decision in this regard by UIIC shall be final and binding on the selected vendor.
- The contract and SLA will be subject to internal policies or guidelines of UIIC and instructions/guidelines etc. as issued by Insurance Regulatory and Development Authority and other Government/Authorities from time to time as applicable.
- The terms of the RFP mentioned across this document shall form part of the agreement.
- The detailed terms and conditions governing the contract shall be included in the Agreement and Service Level Agreement which shall be shared with selected vendor at an appropriate time.
- Selected vendor shall be required to put in place necessary security and all possible safeguards to maintain necessary confidentiality of data and/or information received in any form from UIIC. The selected vendor shall be required to submit the details of all safeguards in place at its facility before commencement of the proposed activity.
- The selected vendor shall have to abide by UIIC Information Security Policy for the activities that shall be carried out for UIIC. This policy & procedures is almost aligned to requirements of ISO 27001 standards (ISMS).
- The SLA between UIIC & selected vendor will have these security controls & liabilities of the selected vendor for violation of UIIC IT & IS policy, standards & procedures.

13.2. Business Continuity

Vendor should have business continuity plan. In case the vendor does not have ready business continuity plan, he should undertake to implement business continuity plan within 3 months from the date of contract. (Proof & Level - ISO 22301)

13.3. Transition Management

Successful Bidder shall provide the Board with a recommended exit management plan ("Exit Management Plan") 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.

- A detailed program of the transfer process that could be used in conjunction with a Replacement Vendor 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;

- Plans for the communication with such of the Successful 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;
- Plans for provision of contingent support to Project and Replacement Vendor for a reasonable period (minimum one month) after transfer.

Successful Bidder shall re-draft the Exit Management Plan annually thereafter to ensure that it is kept relevant and up to date. Each Exit Management Plan shall be presented by the Successful Bidder to UIIC. The terms of payment as stated in the Terms of Payment Schedule include the costs of the Successful Bidder complying with its obligations under this Schedule. During the exit management period, the Successful Bidder shall use its best efforts to deliver the services. Payments during the Exit Management period shall be made in accordance with the Terms of Payment Schedule. This Exit Management plan shall be furnished in writing to Successful Bidder or its nominated agencies within 7 days from the receipt of notice of termination or three months prior to the expiry this Agreement.

13.4. Closure

Upon completion of the contract period, the Vendor will perform all activities necessary to close out the Project. This includes:

- Performing formal contract closure
- Updating process documentation and transferring this to UIIC
- Transitioning any relevant process and/or solution responsibilities over to UIIC, or to another contracted vendor. This includes updating and transferring all solution documentation, performing formal contract closure, and transitioning any relevant solution responsibilities.

13.4.1. After Termination

On termination of the contract the Vendor must:

- stop work on the Services
- deal with UIIC Material as directed by UIIC; and
- return all UIIC's Confidential Information to UIIC

13.5. Termination

13.5.1. Termination for Default

UIIC may, without prejudice to any other remedy for breach of contract by written notice of default sent to the Vendor/Bidder, terminate the contract in whole or in part:

- If the Vendor/Bidder fails to deliver any or all of the services within the time period(s) specified in the contract, or any extension thereof granted by UIIC, OR
- If the Vendor/Bidder fails to perform any other obligation(s) under the contract and fails to remedy the same within 30 days of notice.
- The progress made by the selected Vendor/Bidder is found to be unsatisfactory and fails to remedy the same within 30 days of notice.

UIIC reserves the right to recover any dues payable by the Vendor/Bidder from any amount outstanding to the credit of the Vendor/Bidder, including the pending bills and security deposit, if any, under this contract or any other contract/order.

In the event UIIC terminates the contract in whole or in part, pursuant to above mentioned clause, UIIC may procure, upon such terms and in such manner, as it deems appropriate, services similar to those undelivered. However, the Vendor/Bidder shall continue performance of the contract to the extent not terminated. UIIC shall pay Vendor/Bidder for services performed till effective date of termination.

13.5.2. Termination for Insolvency

UIIC may terminate the agreement without notice and without compensation, if the Vendor/Bidder becomes bankrupt or otherwise admitted into Corporate Insolvency Liquidation Process provided that such termination will-not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to UIIC.

13.5.3. Termination for Convenience

UIIC may send by 30 calendar days' written notice to the Vendor/Bidder to terminate the contract, in whole or in part at any time at its convenience. The notice of termination shall specify the extent to which performance of work under the contract is terminated, and the date upon which such termination becomes effective. In the event of the Vendor/Bidder terminating this agreement, the Vendor/Bidder may send by 90 calendar day's written notice to UIIC to terminate the contract, in whole or in part at any time of their convenience. The notice of termination shall specify the extent to which performance of work under the contract is terminated, and the date upon which such termination becomes effective.

13.5.4. Force Majeure

- The parties shall not be liable for default or non-performance of the obligations under the contract, if such default or non-performance of the obligations under this contract is caused by Force Majeure.

- For the purpose of this clause, "Force Majeure" shall mean an event beyond the control of the parties, due to or as a result of or caused by acts of God, wars, insurrections, riots, earth quake and fire, events not foreseeable but does not include any fault or negligence or carelessness on the part of the parties, resulting in such a situation.
- In the event of any such intervening Force Majeure, each party shall notify the other party in writing of such circumstances and the cause thereof immediately within five calendar days. Unless otherwise directed by the other party, the party pleading Force Majeure shall continue to perform/render/discharge other obligations as far as they can reasonably be attended/fulfilled and shall seek all reasonable alternative means for performance affected by the Event of Force Majeure.
- In such a case, the time for performance shall be extended by a period(s) not less than the duration of such delay. If the duration of delay continues beyond a period of three months or if the parties foresee that the duration of delay would continue for a period of three months or more, the parties shall hold consultations with each other in an endeavour to find a solution to the problem.
- The end of Force Majeure shall be informed to the other party by writing as soon as possible and resume its obligations under this agreement.
- Notwithstanding the above, the decision of UIIC shall be final and binding on the Vendor/Bidder.

13.6. Survival

The following clauses survive the termination and expiry of the contract:

- Clause #1.28(Intellectual Property Rights);
- Clause #1.11 (Indemnity);
- Clause #1.8 (Insurance);
- Clause #1.37 (Non-disclosure);
- Clause #1.7 (Protection of personal information);
- Clause #1.42 (IT & IS Guideline);
- Clause #1.56 (Right to Audit);

13.7. Protection of personal information

This clause applies only where the Vendor deals with personal information when, and for the purpose of, providing Services under the contract.

The Vendor acknowledges that it will use or disclose personal information obtained during the course of providing Services under the contract, only for the purposes of the contract. Kindly refer Non-Disclosure Agreement (**Annexure 9**).

13.8. Insurance

OBLIGATION TO MAINTAIN INSURANCE:

In connection with the provision of the Services, the Vendor must have and maintain for the Contract Period, valid and enforceable insurance policies for: Public liability, cyber liability; either professional indemnity or errors and omissions; workers' compensation as required by law.

13.9. Price

The price covers all expenses for solution components, AMC/ATS, L1 & L2 resources excluding GST. There shall be no escalation in the prices once the prices are fixed and agreed to by the UIIC and the Vendor/Bidder. But any benefit arising out of any subsequent reduction in the prices due to reduction in duty & taxes, after the signing of the agreement should be passed on to the Purchaser /UIIC. Any other expenses like delivery of solution component expenses, travel expenses and hotel stay of bidder resources etc., should not be Bourne by UIIC.

13.10. Use of Contract document and Information

The Vendor/Bidder shall not, without UIIC's prior written consent, disclose the contract or any provision thereof, or any specification, design, drawing, pattern, sample or information furnished by or on behalf of UIIC in connection therewith, to any person other than a person employed by the Vendor/Bidder in the performance of the contract. Disclosure to any such employed person shall be made in confidence and shall extend only as far as may be necessary for purposes of such performance.

The Vendor/Bidder shall not without UIIC's prior written consent, make use of any document or information forming a part of this tender except for purpose of performing the contract.

Any document forming a part of the tender, other than the contract itself, shall remain the property of UIIC.

13.11. Indemnity

Subject to Clause (b) below, Vendor/Bidder (the "Indemnifying Party") undertakes to indemnify UIIC (the "Indemnified Party") from and against all losses on account of bodily injury, death or damage to tangible personal property to any person, corporation or other entity (including the Indemnified Party) due to the Indemnifying Party's negligence, Fraud, Gross negligence or wilful default in performance or non-performance under this Agreement. If the Indemnified Party promptly notifies Indemnifying Party in writing of a

third-party claim against Indemnified Party that any Service provided by the Indemnifying Party infringes a copyright, trade secret or Indian patents of any third party, Indemnifying Party will defend such claim at its expense and will pay any costs or damages that may be finally awarded against Indemnified Party.

(A) The Indemnifying Party will not indemnify the Indemnified Party, however, if the claim of infringement is caused by -

i. Indemnified Party's misuse or modification of the Service;
ii. Indemnified Party's failure to use corrections or enhancements made available by the Indemnifying Party;
iii. Indemnified Party's use of the Service in combination with any product or information not owned or developed by Indemnifying Party.
iv. Indemnified Party's distribution, marketing or use for the benefit of third parties of the Service; or
v. Information, direction, specification or materials provided by Indemnified Party, or any third party contracted to it. If any Service is or likely to be held to be infringing, Indemnifying Party shall at its expense and option (1) procure the right for Indemnified Party to continue using it, (2) replace it with a non-infringing equivalent, (3) modify it to make it non-infringing. The foregoing remedies constitute Indemnified Party's sole and exclusive remedies and Indemnifying Party's entire liability with respect to infringement.

(B) The indemnities set out in Clause (a) shall be subject to the following conditions:

i. The Indemnified Party as promptly as practicable, informs the Indemnifying Party in writing of the claim or proceedings and provides all relevant evidence, documentary or otherwise;
ii. the Indemnified Party shall, at the cost of the Indemnifying Party, give the Indemnifying Party all reasonable assistance in the Defense of such claim including reasonable access to all relevant information, documentation and personnel provided that the Indemnified Party may, at its sole cost and expense, reasonably participate, through its attorneys or otherwise, in such Defense;
iii. If the Indemnifying Party does not assume full control over the Defense of a claim as provided in this Article, the Indemnifying Party may participate in such Defense at its sole cost and expense, and the Indemnified Party will have the right to defend the claim in such manner as it may deem appropriate, and the cost and expense of the Indemnified Party will be included in Losses;
iv. The Indemnified Party shall not prejudice, pay or accept any proceedings or claim, or compromise any proceedings or claim, without the written consent of the Indemnifying Party;
v. All settlements of claims subject to indemnification under this Clause will:
vi. Be entered into only with the consent of the Indemnified Party, which consent will not be unreasonably withheld and include an unconditional release to the

Indemnified Party from the claimant or plaintiff for all liability in respect of such claim; and (b) include any appropriate confidentiality agreement prohibiting disclosure of the terms of such settlement;

vii. The Indemnified Party shall account to the Indemnifying Party for all awards, settlements, damages and costs (if any) finally awarded in favour of the Indemnified Party which are to be paid to it in connection with any such claim or proceedings;

viii. The Indemnified Party shall take steps that the Indemnifying Party may reasonably require to mitigate or reduce its loss as a result of such a claim or proceedings;

ix. In the event that the Indemnifying Party is obligated to indemnify an Indemnified Party pursuant to this Article, the Indemnifying Party will, upon payment of such indemnity in full, be subrogated to all rights and defences of the Indemnified Party with respect to the claims to which such indemnification relates; and

x. If a Party makes a claim under the indemnity set out under Clause 1.11(A) above in respect of any particular Loss or Losses, then that Party shall not be entitled to make any further claim in respect of that Loss or Losses (including any claim for damages).

The Vendor/Bidder shall also indemnify the Purchaser against all third-party claims of infringement of patent, trademark or industrial design rights or any other Intellectual Property Rights, arising from the use of the service or any part thereof (IPR).

Note- The liability arise out of this clause shall exclude liability from the section 1.12 "Limitation of Liability" below.

13.12. Limitation of Liability

Limitation shall not apply to liability arising as a result of Vendor/Bidder's fraud, gross negligence, or wilful misconduct in the performance of the services hereunder.

The liability of Vendor/Bidder (whether in contract, tort, negligence, strict liability in tort, by statute or otherwise) for any claim in any manner related to this Agreement, including the work, deliverables or Services covered by this Agreement, shall be the payment of direct damages only which shall in no event exceed one time the total contract value payable under this Agreement. The liability cap given under this Clause shall not be applicable to the liability arising out of indemnification obligations set out above in 1.11.

Limitation of liability is only with respect with the Vendor/Bidder's liability towards procuring entity and limitation shall not apply with respect to Vendor/Bidder's liability towards third parties.

In no event shall either party be liable for any consequential, incidental, indirect, special, or punitive damage, loss or expenses (including but not limited to business interruption, lost business, lost profits, or lost savings) even if it has been advised of their possible existence.

13.13. Unlimited Liability

The bidder's aggregate liability in connection with obligations, undertaken as a part of this project regardless of the form or nature of the action giving rise to such liability, shall be limited to the Total Cost of Ownership (TCO) of the project. The bidder's liability in case of third-party claims against the UIIC resulting from breach of confidentiality, Wilful Misconduct, or Gross Negligence of the bidder, its employees, and subcontractors or third-party claims resulting from infringement of patents, trademarks, copyrights, or such other Intellectual Property Rights shall be unlimited.

13.14. Professional Liability

The Vendor/Bidder is expected to carry out its assignment with due diligence and in accordance with prevailing standards of the profession. The Vendor/Bidder will cooperate fully with any legitimately provided / constituted investigative body, conducting inquiry into processing or execution of the consultancy contract / any other mater related with discharge of contractual obligation.

13.15. Amendments to this RFP

Amendments to the RFP may be issued by UIIC during the RFP process as required. Amendments to RFP so made shall be deemed to form an integral part of the RFP.

13.16. Contract Amendment

No variation in or modification of the terms of the contract shall be made except by written amendment signed by the parties.

13.17. Format and Signing the Proposals Submitted

The original and all copies of bid proposal submitted by the participant(s) shall be typed or printed in a clear typeface. An accompanying letter is required, signed by an authorized signatory of the participant(s), committing the participant(s) to the contents of the original response. All pages in the bid should be authenticated by a duly authorized signatory of the participant(s) under seal.

13.18. Participant(s) indication of Authorization to Bid

Responses submitted by participant(s) to this RFP represent a firm offer to contract on the terms and conditions described in the participant(s) response. The proposal must be signed by an official authorized to commit the participant(s) to the terms and conditions of the proposal. The signatory should have the authority to sign the documents.

13.19. Language of the Proposals

- All bids and supporting documentation shall be submitted in English.
- The agreement shall be written in English, as specified by UIIC in the instructions to Vendor/Bidder's subject to Section of the RFP. all correspondence and documents relating to the contract and exchanged by the Vendor/Bidder and UIIC, shall be written in English. Any printed literature furnished by the Vendor/Bidder may be written in another language as long as the same is accompanied by an English translation in which case, for the purposes of interpretation of the contract, the English version shall prevail.

13.20. Completeness of the Proposals

The participant's proposal is subject to an evaluation process. Therefore, it is important that the participant(s) carefully prepares the proposal and answers questionnaire completely. The quality of the participant(s) proposal will be viewed as an indicator of the participant(s) capability to provide the solution and participant(s) interest in the project. The participant(s) is required to respond to the RFP only in the prescribed format. Under no circumstances, should the format be changed, altered and modified. All pages including all supporting documents in the bid should be authenticated by a duly authorized signatory of the Participant(s) under seal.

13.21. Acceptance or Rejection of the Proposals

UIIC reserves the right to accept or reject any bid at its sole discretion without assigning any reason whatsoever and the decision of UIIC will be treated as final. The RFP responses/bids/proposals not submitted in the prescribed format or incomplete in any sense are likely to be rejected.

13.22. RFP Ownership

The RFP and all supporting documentation/templates/annexures are the sole property of UIIC and violation of this will be a breach of trust and UIIC would be free to initiate any action deemed appropriate. The bids submitted by the Participants shall be the property of UIIC.

13.23. Preference to "Make in India"

In the tendering process, UIIC will follow the guidelines on Public Procurement (Preference to Make in India), Order 2017 (PPP-MII Order) issued by GOI, Ministry of Commerce and Industry, Department of Industrial Policy and Promotion Letter No. P45021/2/2017(BE-II) dated May 29, 2019, revised on 04-06-2020, further revised on 16-09-2020.

Salient features of the order are given below:

- 'Class-I Local supplier' means a supplier or service provider, whose products or service offered for procurement, has local content equal to or more than 50%, as defined in the above-mentioned order.
- Class-II Local supplier' means a supplier or service provider, whose product or service offered for procurement, has local content more than 20% but less than 50%, as defined in this order.
- 'Non-Local supplier' means a supplier or service provider, whose product or service offered for procurement, has local content less than or equal to 20%, as defined in this order.
- 'Local content' means the amount of value added in India which shall, unless otherwise prescribed by the Nodal Ministry, be the total value of the item procured (excluding net domestic Indirect taxes) minus the value of imported content in the item (including all customs duties) as a proportion of the total value, in percent.

Certificate for local Content: The 'Class-I Local supplier' / 'Class-II Local supplier' shall provide a Certificate from the statutory auditor or cost auditor of the company (in case of companies) or from a practicing cost accountant or practicing chartered accountant (in respect of suppliers other than companies) giving the percentage of local content, on their letter head with Registration Number with seal as per Annexure 19.

13.24. Conflict of Interest

The Vendor/Bidder shall avoid any conflict of interest while discharging contractual obligations and bring, before- hand, any possible instance of conflict of interest to the knowledge of the UIIC, while rendering any advice or service.

The Vendor/Bidder will keep in view transparency, competitiveness, economy, efficiency and equal opportunity to all prospective tenderers / bidders, while rendering any advice / service to UIIC, in regard with matters related to selection of technology and determination of design and specifications of the subject matter, bid eligibility criteria and bid evaluation criteria, mode of tendering, tender notification, etc.

The Vendor/Bidder shall provide professional, objective and impartial advice and at all times hold the UIIC's interest paramount, without any consideration for future work, and that in providing advice they avoid conflicts with other assignment and their interests.

The Vendor/Bidder will ensure adequate accountability, suitable tender terms and conditions for apportioning accountability. Also, there should be suitable provisions to enforce such accountability, in case of improper discharge of contractual obligations / deviant conduct by/ of any of the parties to the contract.

The Vendor/Bidder must act, at all times, in the interest of the UIIC and render any advice/ service with professional integrity. A Vendor/Bidder is expected to undertake an assignment/ project, only in areas of its expertise and where it has capability to deliver efficient and effective advice / services to the UIIC.

13.25. Arbitration Clause

- UIIC and the Vendor/Bidder shall make every effort to resolve amicably by direct informal negotiation, any disagreement or dispute, arising between them under or in connection with the contract.
- If, after thirty (30) days from the commencement of such informal negotiations, UIIC and the Vendor/Bidder have been unable to resolve amicably a contract dispute, either party may require that the dispute be referred for resolution to the formal mechanism specified below.
- In the case of a dispute or difference arising between UIIC and the Vendor/Bidder relating to any matter arising out of or connected with this contract, such dispute or difference shall be referred to a sole arbitrator mutually appointed by the parties. In case sole arbitrator is not agreed by both the parties, then guidelines provided in Arbitration and Conciliation Act, 1996 will be followed.
- The Arbitration and Conciliation Act, 1996, the rules there under and any statutory modification or re- enactments thereof, shall apply to the arbitration proceedings. The seat of arbitration shall be Chennai.
- The contract shall be interpreted in accordance with the Indian Laws for the time being enforced and will be subject to the exclusive jurisdiction of Courts at Chennai (with the exclusion of all other Courts).

13.26. Consortiums or sub-contractor

No consortium bidding and sub-contract is allowed. UIIC will not consider joint or collaborative proposals that require a contract with more than one prime Vendor.

Bidders need to fulfil all the eligibility criteria and technical evaluation criteria in its individual capacity unless mentioned otherwise.

13.27. Cost of the Proposal

All costs relating to preparation, submission of its proposal, attending the clarification sessions and bid opening as well as arranging for the Technical Presentation, cost of POC will be borne by the participant and UIIC will not be responsible or liable, in any way, for any such costs, regardless of the conduct or outcome of the process.

13.28. Intellectual Property Rights

13.28.1. Rights in Vendor's Pre-existing IPR

There shall be no assignment or transfer of any Vendor's pre-existing IPRs (including any amendments, modifications, or enhancements thereto) pursuant to this Agreement.

13.28.2. UIIC ownership of Intellectual Property Rights in RFP

- Within the scope of the RFP, it is stipulated and understood that UIIC will be sole proprietorship of all intellectual property entitlements associated with any logic, design, software, and/or systems meticulously customized for utilization within the scope of work of UIIC, including any reproductions of the design solutions.
- It is binding upon the bidder to guarantee the utmost safeguarding of UIIC's interests and to hold UIIC harmless against any legal repercussions, claims, or third-party liabilities brought forth by any external parties because of utilizing software, designs, or processes furnished by the bidder.

13.29. Solicitation of Employees

Participant(s) will not hire employees of UIIC or solicit or accept solicitation (either directly, indirectly, or through a third party) from employees of UIIC directly involved in this contract during the period of the contract and one year thereafter, except as the parties may agree on a case-by-case basis.

13.30. Liquidated Damages

If the Vendor/Bidder fails to deliver and install the Solution or to perform the services within the time period(s) specified in the contract, UIIC shall without prejudice to its other remedies under the contract, deduct from the contract price, as liquidated damages, a sum equivalent to the 1% of the contract price of the corresponding stage as in TCO for every week (seven days) or part thereof of delay, up to maximum deduction

of 10% of the contract price of the stage. Once the maximum is reached, UIIC may have the sole option to termination of the contract.

The liquidated damage is an estimate of the loss or damage that UIIC may have suffered due to non-performance of any of the obligations (under the terms and conditions) or delay in performance during the contract relating to activities agreed to be undertaken by the Vendor/Bidder and the Vendor/Bidder agrees to dispense with the production of actual proof for any loss suffered by UIIC.

Liquidated damages are not applicable for reasons attributable to UIIC and Force Majeure. However, it is the responsibility/onus of the Vendor/Bidder to prove that the delay is attributed to UIIC and Force Majeure. The Vendor/Bidder shall submit the proof authenticated by the Vendor/Bidder and UIIC's official that the delay is attributed to UIIC and Force Majeure along with the bills requesting payment.

NOTE: The maximum deduction at any point during the project should not surpass 10% of the total contract value.

13.31. Assignment

The vendor/bidder shall not assign, in whole or in part, his obligations to perform under the contract, to any other party or persons except with UIIC's prior written consent.

13.32. Payment Terms

The term of the contract will be for 60 months. The Vendor/Bidder must accept the payment terms and conditions as mentioned in the RFP document.

13.33. Currency of Payments

Payment shall be made in Indian Rupees (INR) only.

13.34. Security Deposit/ Performance Bank Guarantee

1.34.1 Within 15 days of the receipt of Letter of Intent from UIIC, the bidder shall furnish amount equivalent to 5% of the contract value as specified in RFP in the form of irrevocable Bank Guarantee / DD issued by Nationalized/Scheduled Bank towards performance security in accordance with the conditions of contract. UIIC shall provide the pro forma for performance security to the successful bidder.

1.34.2 Performance security shall be valid for 63 months from the date of Letter of Intent.

1.34.3 Failure of the bidder to comply with the requirement of shall constitute sufficient grounds for the annulment of the award and blacklisted for further bidding of future tender/procurement process for 5 years.

1.34.4 In case Bidder after appointment as System Integrator in UIIC refuses to participate or does not participate or does not respond to the requests / RFPs sent by UIIC to them for submission of RFPs and execution of the awarded System Integrator jobs, UIIC may forfeit performance security.

13.35. Variation of Scope

UIIC may at any time during the period of contract, by a written communication to the Vendor/Bidder shall propose modifications within the general scope of the contract for the services provided by the Vendor/Bidder as long as the aforesaid modifications have no impact on commercials and are mutually agreed by both parties.

13.36. Notices

Any notice by one party to the other pursuant to the contract shall be sent in writing or e-mail and confirmed in writing to the address specified for that purpose in the contract. A notice shall be effective when delivered or on the notice's effective date, whichever is later.

13.37. Non-Disclosure

Participant(s) should adhere to non-Disclosure agreement guidelines as described in Annexure 09.

13.38. Tools and Equipment

The Vendor/Bidder shall provide all necessary tools and equipment required for project management under the scope of the project.

Whatever tools and equipment's as deemed fit by the Vendor/Bidder to ensure deliverables as per the RFP, need to be deployed by the Vendor/Bidder.

13.39. Supervision

The Vendor/Bidder shall ensure that all activities are carried out under the direct supervision of qualified / certified personnel.

13.40. Personnel

13.40.1. Use of Specified Personnel

The Vendor will provide the Services or any part of the Services to which their particular experience relates, with the active involvement of, and using the skill of the Specified Personnel; and

Ensure that each of the Specified Personnel is aware of and complies with the Vendor's obligations in providing the Services.

13.40.2. If the Specified Personnel are not available

Where one or more of the Specified Personnel is or will become unable or unwilling to be involved in providing the Services, the Vendor will notify UIIC immediately. The Vendor will:

- If requested by UIIC, provide a replacement person of suitable ability and qualifications, having appropriate technical qualifications and experience equivalent or more than the replaced person, at no additional charge and at the earliest opportunity; and
- Obtain UIIC's written consent prior to appointing any such replacement person.
- Absence of the designated individual on scheduled working days/shifts except on Public holidays specified by UIIC, will incur penalty on per day basis.
- If a deployed resource in this project resigns from the organization, the vendor must promptly inform the UIIC SPOC about the resource's notice period, ensuring the departing resource facilitates a thorough transition and knowledge transfer to their replacement, including all necessary documentation.

13.40.3. UIIC may request replacement of Personnel

UIIC may at any time request the Vendor to remove from work any of the Specified Personnel. The Vendor must promptly arrange for the removal of such Personnel and their replacement in accordance with the process outlined.

13.41. Publicity

Any publicity including but limited to promotions, advertising etc. by the Vendor/Bidder in which the name of UIIC is to be used, should be done only with the explicit written permission from UIIC.

13.42. IT & IS Guidelines

Participant(s) should adhere to Information Technology & Information Security guidelines (Annexure 21).

13.43. Entire Agreement

The parties agree that the agreement along with the RFP, pre-bid queries and any other document and correspondences between the parties prior to the entering of the agreement shall form an integral part and parcel of the agreement and all clauses of this agreement including the arbitration clause contained herein shall apply to those documents.

13.44. Performance Assessment

13.44.1. Assessment of Services

Each element of the Services is subject to assessment by UIIC or any other party nominated by UIIC against the relevant Performance Criteria.

13.44.2. Notice of non-compliant Services

- If UIIC considers that all or part of the Services does not meet the specifications, UIIC will notify the Vendor within 21 Business Days of assessing the Services against the specifications.
- UIIC will include reasons for the Services not meeting the specifications in the notice as given above.

13.44.3. Rectification of non-compliant Services

If UIIC notifies the Vendor that all or part of the Services does not meet the Performance Criteria, the Vendor will:

a. Take all necessary steps to ensure that the Services are promptly corrected.
b. Give notice to UIIC when the Services have been corrected; and
c. Allow UIIC / any other party nominated by UIIC, to repeat the assessment of all or part of the Services against the specifications, within five Business Days after the date of the notice or such other time as agreed mutually.

13.45. Option to extend Contract Period

- The Contract Period may be extended by UIIC on the same terms and conditions mutually agreeable by both the parties, by giving written 30 days' notice to the Vendor.
- Any extension exercised in accordance with the contract takes effect from the end of the then current Contract Period.

13.46. Service Location

Obligation to provide Services: The vendor offers to provide the Services at any location in India as may be required by UIIC.

13.47. General obligations of the parties

The Selected vendor will, at all times:

- Act reasonably in performing its obligations;
- Diligently perform their respective obligations; and
- Work together with UIIC in a collaborative manner.

13.48. Obligations of the selected vendor

The Vendor will supply the Services:

- With due skill and care and to the best of the Vendor 's knowledge and experience;
- In accordance with relevant Indian industry standards, good industry practice and guidelines or where none apply, relevant international industry standards, best practice and guidelines;
- Using the Specified Personnel;

i. Vendor should comply with all the regulatory laws;

ii. The Vendor will be obliged to work closely with UIIC's staff, act within its own authority and abide by directives issued by UIIC and undertake implementation activities.

iii. The Vendor will abide by the job safety measures prevalent in India and will free UIIC from all demands or responsibilities arising from accidents or loss of life the cause of which is the Vendor's negligence. The Vendor will pay all indemnities arising from such incidents and will not hold UIIC responsible or obligated.

iv. The Vendor will be responsible for managing the activities of its personnel and will hold itself responsible for any misdemeanours.

v. In accordance with any reasonable directions in relation to the Services given by UIIC from time to time.

vi. So as to meet the Milestones and other project plan requirements, and where no Milestones or project plan requirements are specified, promptly and without delay.

13.49. Warranties

The Vendor will have to represent and warrant that:

- It has the right to enter into the Contract resulting this RFP;
- It has all rights, title, licenses, interests and property necessary to lawfully perform the Services;
- Its Personnel, including its Specified Personnel, have the necessary experience, skill, knowledge and competence to perform the Services;
- The Services will be complete, accurate and free from material faults; and

- It will not, nor will allow any third party under its direction or control to negligently introduce any Harmful Code into UIIC's systems or Deliverables.

13.50. Cyber Liability

The Bidder shall ensure its compliance with all statutory, regulatory, contractual, and internal policy obligations applicable to this RFP. Examples include but are not limited to INFORMATION TECHNOLOGY ACT, 2000, Information Technology (Amendment) Act, 2008, Regulations under Information Technology Act, IRDAI Cyber Security guidelines. Bidder shall timely update its processes as applicable standards evolve.

13.51. Land Border Restriction

UIIC shall follow the Public procurement guidelines as stipulated in Order ref: 6/18/2019-PPD Dated 23.07.2020 from Department of Expenditure, Ministry of Finance-Restrictions under Rule 144 (xi) of General Financial Rules 2022.

13.52. MSME Waiver

1. If the bidder is a Micro or Small Enterprise as per latest definitions under MSME rules, the bidder shall be exempted from the requirement of "Bidder Turnover" criteria and "Experience Criteria" subject to meeting of quality and technical specifications. If the bidder is OEM of the offered products, it would be exempted from the "OEM Average Turnover" criteria also subject to meeting of quality and technical specifications. In case any bidder is seeking exemption from Turnover / Experience Criteria, the supporting documents to prove his eligibility for exemption must be uploaded for evaluation by the buyer.
2. The minimum average annual financial turnover of the bidder during the last three years, ending on 31st March of the previous financial year, should be as indicated above in the bid document. Documentary evidence in the form of certified Audited Balance Sheets of relevant periods or a certificate from the Chartered Accountant / Cost Accountant indicating the turnover details for the relevant period shall be uploaded with the bid. In case the date of constitution / incorporation of the bidder is less than 3-year-old, the average turnover in respect of the completed financial years after the date of constitution shall be taken into account for this criteria.
3. Years of Past Experience required: The bidder must have experience for number of years as indicated above in bid document (ending month of March prior to the bid opening) of providing similar type of services to any Central / State Govt Organization / PSU / Public Listed Company. Copies of relevant contracts / orders to be uploaded along with bid in support of having provided services during each of the Financial year.
4. Purchase preference to Micro and Small Enterprises (MSEs): Purchase preference will be given to MSEs as defined in Public Procurement Policy for Micro and Small Enterprises (MSEs) Order, 2012 dated 23.03.2012 issued by Ministry of Micro, Small and Medium Enterprises and its subsequent Orders/Notifications issued by concerned

Ministry. If the bidder wants to avail the Purchase preference for services, the bidder must be the Service provider of the offered Service. Relevant documentary evidence in this regard shall be uploaded along with the bid in respect of the offered service. If L-1 is not an MSE and MSE Service Provider (s) has/have quoted price within L-1+ 15% of margin of purchase preference /price band defined in relevant policy, then 100% order quantity will be awarded to such MSE bidder subject to acceptance of L1 bid price. OM_No.1_4_2021_PPD_dated_18.05.2023 for compliance of Concurrent application of Public Procurement Policy for Micro and Small Enterprises Order, 2012 and Public Procurement (Preference to Make in India) Order, 2017.

5. Estimated Bid Value indicated above is being declared solely for the purpose of guidance on EMD amount and for determining the Eligibility Criteria related to Turn Over, Past Performance and Project / Past Experience etc. This has no relevance or bearing on the price to be quoted by the bidders and is also not going to have any impact on bid participation. Also this is not going to be used as a criteria in determining reasonableness of quoted prices which would be determined by the buyer based on its own assessment of reasonableness and based on competitive prices received in Bid / RA process.

13.53. Startup India

The condition of prior turnover and prior experience may be relaxed for Startups (Rule 173 (i) of GFR 2017) (as defined by Department of Industrial Policy and Promotion) subject to meeting of quality & technical specifications and making suitable provisions in the bidding document. The quality and technical parameters are not to be diluted. As defined by Department of Policy & Promotion (DIPP) an entity shall be considered as a 'start-up'-

- Up to ten years from the date of its incorporation/ registration.
- If its turnover for any of the financial years has not exceeded Rs 100 (Rupees Hundred) crore
- It is working towards innovation, development or improvement of products or processes or services, or if it is a scalable business model with a high potential of employment generation or wealth creation
- Provided further that in order to obtain benefits a Startup so identified under the above definition shall be required to be recognized as Startup by DPIIT9.
- As per Department of Expenditure's OM No.F.20/2/2014-PPD dated 20.09.2016, relaxation regarding the prior turnover and prior experience is applicable only to all startups recognized by Department of Industry & Internal Trade (DPIIT) subject to meeting of quality and technical specifications. Startups may be MSMEs or otherwise.

13.54. Right to Audit

Upon notice from UIIC, Vendor shall provide records for inspection and assist UIIC, or its designated third-party contractor, and/ or IRDA and/ or its auditors, if required and

advised by UIIC to Vendor, with access to and any assistance (including financial records, reports and supporting documentation) that they may require with respect to the Service Locations and the Vendor Systems for the purpose of performing audits or inspections of the Services.

13.55. Normalization of Bids

UIIC may, at its sole discretion, decide to seek more information from the respondent in order to normalize the proposals. However, respondents will be notified, if such normalization exercise is resorted to.

Normalization will be done to the extent possible and feasible to ensure that bidders are meeting the requirements of the RFP to the extent possible and that the interest of UIIC is protected.

UIIC reserves the right to normalize any or all of the technical bids. If such normalization has a bearing on the price; UIIC may at its discretion ask the bidders eligible for technical evaluation to submit the technical and commercial bids once again for scrutiny. The submissions can be requested by UIIC in the following two manners:

-Incremental technical bid and / or incremental price submissions in part of the requested clarifications by UIIC OR -Revised technical and / or price submissions of the part or whole bid. The process of normalization may be iterative till such time UIIC is satisfied with the response of the bidders. The bidder by participating in this RFP agrees to the normalization process being followed and adopted by UIIC and has no reservation on the process adopted.

In the event the bidder has any query on the normalization process the same may be raised by the bidder as part of the pre-bid queries.

13.56. Basis for evaluation- QCBS

The basis of overall evaluation will be on a Quality and Cost Based System (QCBS – Offline Mode in E-NIVIDA Portal), for evaluating the tenders.

13.57. Access to UIIC's premises

UIIC will provide the necessary access, to its premises, to the vendor as and when required and is deemed reasonable.

13.58. Conduct at UIIC's premises.

The Selected vendor will, if using or accessing UIIC 's premises or facilities, comply with all reasonable directions and procedures relating to occupational health and safety and security in operation at those premises or facilities whether specifically drawn to the attention of the Vendor or as might reasonably be inferred from the circumstances.

13.59. Miscellaneous

13.59.1. Varying the contract

The contract may be varied only in writing signed by each party.

13.59.2. Approvals and consents

Except where the contract expressly states otherwise, a party may, in its discretion, give conditionally or unconditionally or withhold any approval or consent under the contract.

13.59.3. Assignment and novation

A party may only assign its rights or novate its rights and obligations under the contract with the prior written consent of the other party.

13.59.4. Further action

Each party must do, at its own expense, everything reasonably necessary (including executing documents) to give full effect to the contract and any transaction contemplated by it.

13.59.5. Waiver

Waiver of any provision of or right under the contract:

A. must be in writing signed by the party entitled to the benefit of that provision or right; and
B. is effective only to the extent set out in any written waiver agreed by the other party.

13.59.6. Relationship

A. The parties must not represent themselves, and must ensure that their officers, employees, and agents do not represent themselves, as being an officer, employee, partner or agent of the other party, or as otherwise able to bind or represent the other party.

B. The contract does not create a relationship of employment, agency or partnership between the parties.

13.59.7. Announcements

A. The Vendor must, before making a Public announcement in connection with the contract or any transaction contemplated by it, obtain UIIC's written agreement to the announcement.

B. If the Vendor is required by law or a regulatory body to make a Public announcement in connection with the contract or any transaction contemplated by the contract the Vendor must, to the extent practicable, first consult with and consider the reasonable requirements of UIIC.

13.60. Integrity pact

To ensure transparency, equity, and competitiveness and in compliance with the CVC guidelines, this tender shall be covered under the Integrity Pact (IP) policy of UIIC. The pact essentially envisages an agreement between the prospective bidders/vendors and UIIC committing the persons/officials of both the parties, not to exercise any corrupt influence on any aspect of the contract. The format of the agreement is enclosed in Annexure 12 – Integrity Pact.

Signing of the IP with UIIC would be one of the preliminary qualifications for further evaluation. In other words, entering into this pact would be one of the preliminary qualifications for this tender and the pact shall be effective from the stage of invitation of bids till the complete execution of the contract. Any vendor/bidder not signed the document or refusing to sign shall be disqualified in the bidding process

The Integrity Pact envisages a panel of Independent External Monitors (IEMs) to review independently and objectively, whether and to what extent parties have complied with their obligation under the pact. The IEM has the right to access to all the project documents, Shri Dharam Chand Jain, IPS (Retd.) and Shri Vijay Sharma, IRSE (Retd.), IAS (Retd.) shall be acting as the IEM for this contract/Tender. However, UIIC at its sole discretion reserves the right to change/name another IEM, which shall be notified latter

Contact Details:

Shri Dharam Chand Jain, IPS (Retd.)	Shri Vijay Sharma, IRSE (Retd.)

4F, Type-VII, Tower-6, East Kidwai Nagar, New Delhi – 110023.	Flat no.9112, Parx Laureate, Sector 108, Noida, Uttar Pradesh, 201304.

13.61. Vendor Risk Assessment

The TSP shall implement processes and controls to ensure that risks associated with third-parties (e.g. vendors, contractors, business partners, etc.) providing information technology equipment, software, and/or services are minimized or avoided. Third party management processes and controls shall include, at a minimum:

i. Tailored acquisition strategies, contracting tools, and procurement methods for the purchase of systems, system components, or system service from suppliers;
ii. Due diligence security reviews of suppliers and third parties with access to the Vendor's {TSP's} systems and sensitive information;
iii. Third party interconnection security; and
iv. Independent testing and security assessments of supplier technologies and supplier organizations.

Note- Vendor has to co-ordinate in Vendor Assessment Programme whenever held by UIIC as

ANNEXURE 1- FORMAT FOR LETTER OF AUTHORIZATION

(To be submitted in the Bidder's letter head)

[TO BE INCLUDED IN 'COVER – A' ELIGIBILITY CUM TECHNICAL BID ENVELOPE]

Ref. No: xx

To

The Deputy General Manager
Information Technology Department
United India Insurance Co. Ltd.
Head Office, 24, Whites Road,
Chennai – 600014

LETTER OF AUTHORISATION FOR ATTENDING BID OPENING

The following persons are hereby authorized to attend the bid opening on _____(date) in respect of the tender for "<>" on behalf of M/s._____(Name of the Bidder) in the order of preference given below:

Order of Preference Name Designation Specimen Signature 1.

2.

(Authorized Signatory of the Bidder)

Date:

(Company Seal)

1. Maximum of two persons can be authorized for attending the bid opening.
2. Permission for entry to the hall where bids are opened may be refused in case authorization as prescribed above is not submitted.

ANNEXURE 2-NO BLACKLIST DECLARATION

(To be submitted in the Bidder's letter head)

[TO BE INCLUDED IN 'COVER – A' ELIGIBILITY CUM TECHNICAL BID ENVELOPE]

Ref. No: xx

To
The Deputy General Manager
Information Technology Department
United India Insurance Co. Ltd.
Head Office, 24, Whites Road,
Chennai – 600014

Subject: Submission of No Blacklisting Self-Declaration for Tender Ref. No: <>

Dear Sir/Madam,

We do hereby declare and affirm that we have not been blacklisted/debarred by any Government Departments, Agencies or Public Sector Undertakings in India as on the date of submission of the tender for "<>"

(Authorized Signatory of Bidder)

Date:
(Company
Seal)

ANNEXURE 3A - MANUFACTURERS AUTHORISATION FORMAT

(To be submitted on OEMs Letter Head)

[TO BE INCLUDED IN 'COVER – A' ELIGIBILITY CUM TECHNICAL BID ENVELOPE]

Ref. No: 000100/HO IT/RFP/282/2025-2026

To

The Deputy General Manager
Information Technology Department
United India Insurance Co. Ltd.
Head Office, 24, Whites Road,
Chennai – 600014

Subject: Manufacturers Authorization Form for the "<>"

<This MAF should be on the letterhead of the OEM and should be signed by a person competent and having the power of attorney to bind the manufacturer. It should be included by the bidder in its eligibility bid>

MAF should broadly cover the following:

1. Registered office address of OEM.

2. We, M/s_____ are the OEM of _____(Name of the product/Solution/Hardware), being offered to United India Insurance Company Ltd through M/s _____(Bidder's Name), who is our authorized Partner/representative in India for supply of this Product/Solution/Hardware.

3. We, M/s _____ have the IP (Intellectual property) rights for the products.

4. We agree to provide services as per the scope of work and technical specifications of this RFP through our partner M/s _____

5. Confirm extension of full warranty and guarantee as per the terms and conditions of the tender and the contract for the solution, products/equipment and services including extension of technical support and updates / upgrades if contracted by the bidder.

6. Ensure all product upgrades including software upgrades and new product feature releases during the contract period.

7. And also confirm that such Products as UIIC may opt to purchase from the Supplier, provided, that this option shall not relieve the Supplier of any warranty obligations under the Contract.

8. In the event of termination of production of such Products:

    a. advance notification to UIIC of the pending termination, in sufficient time to permit the UIIC to procure needed requirements; and
    b. Following such termination, furnishing at no cost to UIIC, the blueprints, design documents, operations manuals, standards and specifications of the Products, if requested.

9. In case the bidder i.e. M/s _____ is not able to perform obligations as per RFP during the contract period (like if bidder ceases to exist from the ICT Industry, stops services or support to the UIIC, terminates contract due any reasons with UIIC or due to any other reason), we will perform the said obligations, as per given scope of work of RFP, either directly or through mutually agreed third party/any other authorized Partner of ours at no extra cost to the company.

10. With reference to the all components/parts/assemble/software used inside the company products/Hardware being quoted by us vide your tender cited above, we hereby undertake that all the components / parts / assembly used inside the company products/Hardware shall be original new components / parts / assembly / software only, from respective OEMs of the products and that no refurbished / duplicate / second hand components / parts / assembly are being used or shall be used.

11. In case of default/unable to comply with above at the time of delivery or during implementation, for the IT asset including hardware / software already billed, we agree to take back the supplied items without demur, if already supplied and replace the same with new one.

Yours faithfully,

(Authorized Signatory of Bidder)

Date:

(Company Seal)

ANNEXURE 3B - UNDERTAKING FOR BEING THE OEM OF THE OFFERED SOLUTION

(To be submitted on OEMs Letter Head)

[TO BE INCLUDED IN 'COVER – A' ELIGIBILITY CUM TECHNICAL BID ENVELOPE]

Ref. No: xx

To

The Deputy General Manager

Information Technology Department

United India Insurance Co. Ltd.

Head Office, 24, Whites Road,

Chennai – 600014.

Subject: Undertaking for being the OEM of the offered solution for the "<>"

We hereby submit the following:

1. Registered office address of OEM.

2. We, M/s_____ are the OEM of _____ (Name of the product/Solution/Hardware), being offered to United India Insurance Company Ltd direclty for supply of this Product/Solution/Hardware.

3. We, M/s _____ have the IP (Intellectual property) rights for the products.

4. We agree to provide services as per the scope of work and technical specifications of this RFP

5. Confirm extension of full warranty and guarantee as per the terms and conditions of the tender and the contract for the solution, products/equipment and services including extension of technical support and updates / upgrades if contracted by the bidder.
6. Ensure all product upgrades including software upgrades and new product feature releases during the contract period.

7. In the event of termination of production of such Products:

    a. advance notification to UIIC of the pending termination, in sufficient time to permit

the UIIC to procure needed requirements; and

b. Following such termination, furnishing at no cost to UIIC, the blueprints, design documents, operations manuals, standards and specifications of the Products, if requested.

8. With reference to the all components/parts/assemble/software used inside the company products/Hardware being quoted by us vide your tender cited above, we hereby undertake that all the components / parts / assembly used inside the company products/Hardware shall be original new components / parts / assembly / software only, from respective OEMs of the products and that no refurbished / duplicate / second hand components / parts / assembly are being used or shall be used.

9. In case of default/unable to comply with above at the time of delivery or during implementation, for the IT asset including hardware / software already billed, we agree to take back the supplied items without demur, if already supplied and replace the same with new one.

Yours faithfully,

(Authorized Signatory of Bidder)

Date:

(Company Seal)

ANNEXURE 4 - STATEMENT OF NIL DEVIATIONS

(To be submitted in the Bidder's letterhead)

[TO BE INCLUDED IN 'COVER – A' ELIGIBILITY CUM TECHNICAL BID ENVELOPE]

Ref. <>

To

The Deputy General Manager

Information Technology Department

United India Insurance Co. Ltd.

Head Office, 24, Whites Road,

Chennai – 600014.

Re: Your RFP Ref.<>

Dear Sir,

There are no deviations (nil deviations) from the terms and conditions of the tender. All the terms and conditions of the tender are acceptable to us.

Authorized Signatory Name Designation Office

Seal Place:

Date:

ANNEXURE 5 - BANK GUARANTEE FORMAT FOR EMD

[TO BE INCLUDED IN 'COVER – A' ELIGIBILITY CUM TECHNICAL BID ENVELOPE]

To

The Deputy General Manager

Information Technology Department

United India Insurance Co. Ltd.

Head Office, 24, Whites Road,

Chennai – 600014.

Whereas..... (Hereinafter called "the Bidder") has submitted its bid dated..... (Date of submission of bid) for the "<> "(hereinafter called "the Bid"), we.....(Name of Bank), having our registered office at. (Address of bank) (Hereinafter called "the Bank"), are bound unto United India Insurance Co. Ltd (hereinafter called "the Purchaser") for the sum of ₹ 30,00,000/-(Rupees Thirty Lakh only) for which payment well and truly to be made to the said Purchaser, the Company binds itself, its successors, and assigns by these presents.

THE CONDITIONS of this obligation are:

- If the Bidder/System Integrator withdraws his offer after issuance of letter of Intent by UIIC;
- If the Bidder/System Integrator withdraws his offer before the expiry of the validity period of the tender
- If the Bidder/System Integrator violates any of the provisions of the terms and conditions of this tender specification.
- If a Bidder/System Integrator, who has signed the agreement and furnished Security Deposit backs out of his tender bid.
- If a Bidder/System Integrator having received the letter of Intent issued by UIIC, fails to furnish the bank guarantee and sign the agreement within the 15(Fifteen) days from the letter of Intent.

We undertake to pay the Purchaser up to the below amount upon receipt of its first written demand, without the Purchaser having to substantiate its demand, provided that in its demand the Purchaser will note that the amount claimed by it is due to it, owing to the occurrence of all/any of the above conditions, specifying the occurred condition or conditions.

This guarantee will remain in force up to and including ninety (90) days from last date of bid submission, and any demand in respect thereof should reach the Company not later than the above date. Notwithstanding anything contained herein:

1. Our liability under this bid security shall not exceed₹ 30,000/-
2. This Bank guarantee will be valid up to.....(Date);
3. We are liable to pay the guarantee amount or any part thereof under this

Bank guarantee only upon service of a written claim or demand by you on or before .....(Date).

In witness whereof the Bank, through the authorized officer has set its hand and stamp on this……. day of …….at ……..

(Signature of the Bank)

NOTE:

1. Bidder should ensure that the seal and CODE No. of the authorized signatory is put by the bankers, before submission of the bank guarantee.
2. Bank guarantee issued by banks located in India shall be on a Non-Judicial Stamp Paper of appropriate value.
3. Bid security should be in INR only.
4. Presence of restrictive clauses in the Bid Security Form such as suit filed clause/ requiring the Purchaser to initiate action to enforce the claim etc., will render the Bid non-responsive.

Unsuccessful bidders' bid security will be discharged or returned after the expiration of the period of bid validity prescribed by the Company.

The successful bidder's bid security will be discharged upon the bidders signing the contract and furnishing the performance bank guarantee.

ANNEXURE 6 - ELIGIBILITY CRITERIA FORM

[TO BE INCLUDED IN 'COVER – A' ELIGIBILITY CUM TECHNICAL BID ENVELOPE]

To

The Deputy General Manager
Information Technology Department
United India Insurance Co. Ltd.
Head Office, 24, Whites Road,
Chennai – 600014.

Ref. 000100/HO IT/RFP/282/2025-2026

ELIGIBILITY CRITERIA FOR BIDDERS

S.No.	Particulars	
1	Registered Name & Address of The Bidder	
2	Location of Corporate Head Quarters	
3	Date & Country of Incorporation	
4	GSTIN and date of registration	
5	In the Location business since (year)	
6	Whether the bidder is an OEM / SI	
7	Address for Communication	
8	Contact Person-1 (Name, Designation, Phone, Email ID)	
9	Contact Person-2 (Name, Designation, Phone, Email ID)	

TURN OVER & NET PROFIT

Financial Year / Accounting Year	Turnover (in Crores)	Net Profit
2021-2022		
2022-2023		
2023-2024		

Eligibility Criteria

#	Eligibility Criteria for Bidders	Documentary Proof Required
1	The Bidder should be a Registered Company in India under the 'Companies Act' and should be in business in India for more than ten years as on 31.03.2025.	Copy of the Certificate of Incorporation issued by Registrar of Companies.
2	The bidder should have an average annual financial turnover of at least ₹500 Crore for the last three financial years' viz. 2021-2022, 2022-2023, and 2023-2024. For startups and MSMEs, the average annual financial turnover should be at least ₹50 Crore for the last three financial years' viz. 2021-2022, 2022-2023, and 2023-2024.	Audited financial statements / Certificate from Auditor.
3	Bidder must have net profit in any of the two years during the last three completed financial years - 2021-2022, 2022-2023, and 2023-2024.	Audited financial statements / Certificate from Auditor.
4	The bidder should not have been blacklisted/ debarred by any Government Departments, Agencies or Public Sector Undertakings in India as on the date of submission of the tender.	As per Annexure 2: No Blacklist declaration
5	The bidder must have its own support centers or offices in at least ten (10) locations across Tier 1 and Tier 2 cities out of which mandatorily should be in Mumbai, Hyderabad and Chennai to provide telephonic and remote assistance services. In case of exigencies or onsite support requirements at various branch locations of	Self-Declaration along with the details of the support centers and service locations across India must be submitted as part of the bid.

#	Eligibility Criteria for Bidders	Documentary Proof Required
	UIIC across India, the bidder shall arrange timely support.	
6	During the last 5 years, the bidder should have supplied, implemented, and supported the below tools for clients in PSU /Government organization /BFSI within India. • Data Loss Prevention (DLP), • Endpoint Detection and Response (EDR), • Data discovery and Data classification For each of the above tools, a minimum of two (02) references to be provided, out of which one should be of proposed OEM. The minimum deployment size required is as follows: • For Startups and MSMEs: Minimum 3000 endpoints for each tool • For rest of the bidders: Minimum 5000 endpoints for each tool	Bidder should Provide Purchase Order(s) with the performance certificate as per Annexure 18 signed & sealed by the respective Bidder's customers along with their contact details (email, mobile and landline). UIIC reserve the rights to directly interact with any of the contact submitted.
7	During the last 5 years, the proposed OEM should have been implemented for minimum two (02) clients with at least one in PSU /Government organization /BFSI within India. • Data Loss Prevention (DLP) for minimum 10000 endpoints, • Endpoint Detection and Response (EDR) for minimum 10000 endpoints, • Data discovery and Data classification for minimum 10000 endpoints,	Bidder should Provide Purchase Order(s) with the performance certificate as per Annexure 18 signed & sealed by the respective Bidder's customers along with their contact details (email, mobile and landline). UIIC reserves the right to directly interact with any of the contact submitted.

#	Eligibility Criteria for Bidders	Documentary Proof Required
	• Mobile Device Management (MDM) for minimum 2000 endpoints, • Patch Management Solution for minimum 10000 endpoints, • Key Management Solution for BitLocker key.	
8	The bidder should have deployed a minimum of at least 10 (L1 & L2) OEM certified resources/ personnels for the Proposed /Similar solutions in scope for at least one (01) PSU/ Government /BFSI client (and) Bidder should have at least 10 personnel (OEM certified) out of which 4 personnel certified for any of the proposed OEM on their direct payroll.	Details of such personnel (PO and Invoices mentioning number of resources/FMS) along with copy of OEM certificates required along with declaration stating resources are on payroll.
9	Bidder should submit the Land Border Clause as per Annexure 13.	Bidder needs to Submit Annexure 13 on letter head dully signed by Authorized signatory.

Note:

1. Bidder should submit detailed response along with documentary proof for all of the above eligibility criteria. The eligibility will be evaluated based on the bid and the supporting documents submitted. Bids not meeting the above eligibility criteria will be rejected.
2. Technical Evaluation will be done by UIIC‟s technical evaluation committee and the decision of the committee will be final.
3. Bidders to submit relevant documentary evidence for all parameters mentioned.
4. Providing any wrong information by the bidder will result in disqualification of the bidder. The UIIC may cross check above parameters by any means / during site visit.
5. All Annexures must be on the letter head of the Bidder, except those which are to be provided by OEM/CA/third party/Customer. All documents, addressed to the UIIC, should be submitted in Original and scanned photocopies.

6. All documents must be signed by their authorized signatory of the respective parties and his/her designation, Official E-mail ID and Mobile no. should also be evident. Bidder has to provide the authorization letter evidencing the person signing the document is authorized to do so on behalf of his company. Inability of the bidder to prove the genuineness/authenticity of any third-party document may make the bid liable for rejection.
7. All documents submitted by the bidder should be signed by the authorized signatory. The Bidder also to submit letter from competent authority evidencing delegation of authority to the authorized signatory along with details such as designation, mail id and mobile number.
8. In respect of all other documents adduced by the bidder as evidence substantiating his claims, the same should be signed by the authorized signatories of the respective entities duly self-attested by the bidder authorized signatory.

Authorized Signatory Name Designation Office

Seal Place:

Date:

ANNEXURE 7 - TECHNICAL CRITERIA FORM

[TO BE INCLUDED IN 'COVER – A' ELIGIBILITY CUM TECHNICAL BID ENVELOPE]

#	Technical Evaluation Criteria – Parameters	Maximum Score
1	During the last 5 years bidder should have experience in supplying, implementing and supporting Mobile Device Management (MDM) for a minimum of 2000 endpoints for PSU /Government organization /BFSI client within India. • 2 References -> 0 Marks • Every additional reference -> 2 Marks subjected to maximum 4 marks (Supporting Document: Bidder should Provide Purchase Order(s) with the performance certificate as per Annexure 18 signed & sealed by the respective Bidder's customers along with their contact details (email, mobile and landline)	4
2	During the last 5 years bidder should have experience in supplying, implementing and supporting Patch Management for a minimum of 5000 endpoints for PSU /Government organization /BFSI client within India. • 2 References -> 0 Marks • Every additional reference -> 2 Marks subjected to maximum 4 marks (Supporting Document: Bidder should Provide Purchase Order(s) with the performance certificate as per Annexure 18 signed & sealed by the respective Bidder's customers along with their contact details (email, mobile and landline)	4
3	During the last 5 years bidder should have experience in supplying, implementing and supporting Key Management Solution for BitLocker keys for PSU /Government organization /BFSI client within India. • 1 Reference -> 0 Mark	2

#	Technical Evaluation Criteria – Parameters	Maximum Score
	• 2 References -> 2 Marks (Supporting Document: Bidder should Provide Purchase Order(s) with the performance certificate as per Annexure 18 signed & sealed by the respective Bidder's customers along with their contact details (email, mobile and landline)	
4	During the last 5 years the proposed OEM for Data Loss Prevention (DLP) should have been implemented for a minimum of 10000 endpoints for clients in PSU /Government organization /BFSI within India. • 2 References -> 0 Marks • Every additional reference -> 2 Marks subjected to maximum 4 marks (Supporting Document: Bidder should Provide Purchase Order(s) with the performance certificate as per Annexure 18 signed & sealed by the respective Bidder's customers along with their contact details (email, mobile and landline).	4
5	During the last 5 years the proposed OEM for Data Classification and Data Discovery should have been implemented for a minimum of 10000 endpoints for clients in PSU /Government organization /BFSI within India. • 2 References -> 0 Marks • Every additional reference -> 2 Marks subjected to maximum 4 marks (Supporting Document: Bidder should Provide Purchase Order(s) with the performance certificate as per Annexure 18 signed & sealed by the respective Bidder's customers along with their contact details (email, mobile and landline).	4
6	During the last 5 years the proposed OEM for Extended Detection and Response (EDR) should have been implemented for a minimum	4

#	Technical Evaluation Criteria – Parameters	Maximum Score
	of 10000 endpoints for clients in PSU /Government organization /BFSI within India. • 2 References -> 0 Marks • Every additional reference -> 2 Marks subjected to maximum 4 marks (Supporting Document: Bidder should Provide Purchase Order(s) with the performance certificate as per Annexure 18 signed & sealed by the respective Bidder's customers along with their contact details (email, mobile and landline).	
7	During the last 5 years the proposed OEM for Mobile Device Management (MDM) should have been implemented for a minimum of 10000 endpoints for clients in PSU /Government organization /BFSI within India. • 2 References -> 0 Marks • Every additional reference -> 2 Marks subjected to maximum 4 marks (Supporting Document: Bidder should Provide Purchase Order(s) with the performance certificate as per Annexure 18 signed & sealed by the respective Bidder's customers along with their contact details (email, mobile and landline).	4
8	During the last 5 years the proposed OEM for Patch Management should have been implemented for a minimum of 10000 endpoints for clients in PSU /Government organization /BFSI within India. • 2 References -> 0 Marks • Every additional reference -> 2 Marks subjected to maximum 4 marks (Supporting Document: Bidder should Provide Purchase Order(s) with the performance certificate as per Annexure 18 signed &	4

#	Technical Evaluation Criteria – Parameters	Maximum Score
	sealed by the respective Bidder's customers along with their contact details (email, mobile and landline).	
9	During the last 5 years the proposed OEM for Key Management Solution for BitLocker should have been for clients in PSU /Government organization /BFSI within India. • 2 Reference -> 0 Marks • 4 References -> 4 Marks (Supporting Document: Bidder should Provide Purchase Order(s) with the performance certificate as per Annexure 18 signed & sealed by the respective Bidder's customers along with their contact details (email, mobile and landline)	4
10	Bidder should have OEM certified personnel for in-scope solutions on their direct payroll • Up to 20 certified resources -> 5 Marks • For every additional 5 certified resources -> 5 Marks subjected to maximum 20 marks (Supporting Document: Details of such personnel along with copy of OEM certificates along with declaration stating resources are on payroll)	20
11	Presentation to be made by the Bidder on understanding of the requirements and proposed methodology including but not limited to: • Depth of understanding and relevance of proposed approach and methodology to the scope of work • Demonstrated experience in similar engagements with proven outcomes and domain-specific implementations • Proposed teams' qualifications, certifications, and experience aligned to support the engagement requirements effectively	6

#	Technical Evaluation Criteria – Parameters	Maximum Score
	(60 Minutes presentation which includes demonstration of solutions functionalities)	
12	The OEM's ability to meet Technical Specification (Annexure 10). For each requirement, the OEM has to do self-assessment and update score as either 0, 1 or 2 • 0 – Feature is not feasible. • 1 – Feature is not available as part of the solution but will be provided as part of customization. OEM to provide detailed information about how the customization shall be done. • 2 – Feature is available as part of the solution Scoring out of a maximum of 40 marks can be calculated as below: Score = (Marks obtained / Total Marks) * 40 (rounded off to 3 decimal places)	40
Total		100

ANNEXURE 8 - COMMERCIAL BID FORMAT [ALL AMOUNTS SHOULD BE IN INR]

[To be included in Cover 'B'- Commercial Bid]

To

The Deputy General Manager
Information Technology Department
United India Insurance Co. Ltd.
Head Office, 24, Whites Road,
Chennai – 600014.

Ref. <>

DC-DR SOLUTION COST

#	Component	Solution OEM	Quantity	Year 1		Year 2		Year 3		Year 4		Year 5		Total 5 Year Cost (INR)	Taxes As applicable (INR)	Grand Total (INR)
				Unit Price (INR)	Total Price (INR)	Unit Price (INR)	Total Price (INR)	Unit Price (INR)	Total Price (INR)	Unit Price (INR)	Total Price (INR)	Unit Price (INR)	Total Price (INR)			
1	Hardware		As per scope	x	x	x	x	x	x	x	x	x	x			
2	DLP Software Licenses		As per scope													
3	EDR Software Licenses		As per scope													
4	Data Discovery & Classification Software Licenses		As per scope													
5	MDM For Laptops Software Licenses		As per scope													
6	Patch Management Software Licenses		As per scope													
7	KMS Software Licenses		As per scope													
8	One Time Implementation Cost		One Time	x	x	x	x	x	x	x	x	x	x			
9	Facility Management Services (FMS) - L1 Resource		As per scope													
10	Facility Management		As per													

#	Component	Solution OEM	Quantity	Year 1		Year 2		Year 3		Year 4		Year 5		Total 5 Year Cost (INR)	Taxes As applicable (INR)	Grand Total (INR)
				Unit Price (INR)	Total Price (INR)	Unit Price (INR)	Total Price (INR)	Unit Price (INR)	Total Price (INR)	Unit Price (INR)	Total Price (INR)	Unit Price (INR)	Total Price (INR)			
	Services (FMS) - L2 Resource		scope													
11	Facility Management Services (FMS) - Project Coordinator		As per scope													
12	Annual Maintenance Contract (AMC)		As per scope	x	x	x	x	x	x	x		x				
13	Any Other, (Please specify)															
Grand Total (INR, incl. all components) - A																

PRICE DISCOVERY FOR ADDITIONAL LICENSES

#	Component	Solution OEM	Quantity	Year 1		Year 2		Year 3		Year 4		Year 5		Total 5 Year Cost (INR)	Taxes As applicable (INR)	Grand Total (INR)
				Unit Price (INR)	Total Price (INR)	Unit Price (INR)	Total Price (INR)	Unit Price (INR)	Total Price (INR)	Unit Price (INR)	Total Price (INR)	Unit Price (INR)	Total Price (INR)			
1	DLP Software Licenses		100													
2	EDR Software Licenses		100													
3	Data Discovery & Classification Software Licenses		100													
4	MDM For Laptops Software Licenses		100													
5	Patch Management Software Licenses		100													
6	Any Other, (Please specify)															
Grand Total (INR, incl. all components) - B																

TOTAL PRICE IN WORDS EXCLUSIVE OF TAXES (A + B): _____(in Rs.)

NOTE: All the commercials, with unmasked values, should be submitted along with the Commercial Bid Format.

NOTE:

- The Total Cost of Ownership (TCO) shall be total of the "DC-DR SOLUTION COST" and the cost of "PRICE DISCOVERY FOR ADDITIONAL LICENSES"
- Bidder must propose the additional license cost for the 5 years of contract period in the above format (In case of future requirement)

- The Bidder is expected to provide a detailed break up of all products and services that are under the scope of facilities management as part of the technical bid, in the technical bill of materials i.e. the above format is expected to be replicated for each item to be covered under the scope of facilities management.
- The quantity mentioned above is for price identification purpose only and additional licenses will be procured on actual requirement basis.

Authorized Signatory Name Designation Office Seal

Place:
Date:

ANNEXURE 9 - NDA (NON - DISCLOSURE AGREEMENT FORMAT)

(To be submitted in separate ₹100 stamp paper)

[TO BE INCLUDED IN 'COVER – A' ELIGIBILITY CUM TECHNICAL BID ENVELOPE]

This confidentiality and non-disclosure agreement is made on the.....day of…… ,

20..... between (Bidder), (hereinafter to be referred to as "-------") which expression shall unless repugnant to the subject or the context mean and included its successors, nominees or assigns a company incorporated under the Companies Act, 1956 and having its principal office at .....(address) and UNITED INDIA INSURANCE COMPANY LIMITED (hereinafter to be called "UIIC") which expression shall unless repugnant to the subject or the context mean and included its successors, nominees or assigns having its Registered Office at (address) on the following terms and conditions:

WHEREAS, in the course of the business relationship between the aforesaid parties, both the parties acknowledge that either party may have access to or have disclosed any information, which is of a confidential nature, through any mode and recognize that there is a need to disclose to one another such confidential information, of each party to be used only for the Business Purpose and to protect such confidential information from unauthorized use and disclosure;

NOW THEREFORE, in consideration of the mutual promises contained herein, the adequacy and sufficiency of which consideration is hereby acknowledged and agreed, the parties hereby agree as follows:

This Agreement shall apply to all confidential and proprietary information disclosed by one party to the other party, including information included in the caption 'Definitions' of this Agreement and other information which the disclosing party identifies in writing or otherwise as confidential before or within thirty days after disclosure to the receiving party ("Confidential Information"). Information may be in any form or medium, tangible or intangible, and may be communicated/disclosed in writing, orally, electronically or through visual observation or by any other means to one party (the receiving party) by the other party (the disclosing party).

1. DEFINITIONS

CONFIDENTIAL INFORMATION means all the information of the Disclosing Party which is disclosed to the Receiving party pursuant to the business arrangement whether oral or written or through visual observation or in electronic mode and shall include but is not limited to trade secrets, know-how, inventions, techniques, processes, plans, algorithms, software programs, source code, semiconductor designs, schematic designs, business methods, customer lists, contacts, financial information, sales and

marketing plans techniques, schematics, designs, contracts, financial information, sales and marketing plans, business plans, clients, client data, business affairs, operations, strategies, inventions, methodologies, technologies, employees, subcontractors, the contents of any and all agreements, subscription lists, customer lists, photo files, advertising materials, contract quotations, charity contracts, documents, passwords, codes, computer programs, tapes, books, records, files and tax returns, data, statistics, facts, figures, numbers, records, professionals employed, correspondence carried out with and received from professionals such as Advocates, Solicitors, Barristers, Attorneys, Chartered Accountants, Company Secretaries, Doctors, Auditors, Surveyors, Loss Assessors, Investigators, Forensic experts, Scientists, Opinions, Reports, all matters coming within the purview of Privileged Communications as contemplated under Indian Evidence Act, 1872, legal notices sent and received, Claim files, Insurance policies, their rates, advantages, terms, conditions, exclusions, charges, correspondence from and with clients/ customers or their representatives, Proposal Forms, Claim-forms, Complaints, Suits, testimonies, matters related to any enquiry, claim-notes, defences taken before a Court of Law, Judicial Forum, Quasi-judicial bodies, or any Authority, Commission, pricing, service proposals, methods of operations, procedures, products and/ or services and business information of the Disclosing Party. The above definition of Confidential Information applies to both parties equally; however, in addition, without limitation, where the Disclosing Party is the UIIC, no information that is exempted from disclosure under section8 or any other provision of Right to Information Act, 2005 shall at any time be disclosed by the Receiving Party to any third party.

(a) MATERIALS means including without limitation, documents, drawings, models, apparatus, sketches, designs and lists furnished to the Receiving Party by the Disclosing Party and any tangible embodiments of the Disclosing Party's Confidential Information created by the Receiving Party.

2. COVENANT NOT TO DISCLOSE

The Receiving Party will use the Disclosing Party's Confidential Information solely to fulfil its obligations as part of and in furtherance of the actual or potential business relationship with the Disclosing Party. The Receiving Party shall not use the Confidential Information in any way that is directly or indirectly detrimental to the Disclosing Party or its subsidiaries or affiliates and shall not disclose the Confidential Information to any unauthorized third party. The Receiving Party shall not disclose any Confidential Information to any person except to its employees, authorized agents, consultants and contractors on a need-to-know basis, who have prior to the disclosure of or access to any such Confidential Information agreed in writing to receive it under terms at least as restrictive as those specified in this Agreement.

In this regard, the agreement entered into between the Receiving Party and any such person/s shall be forwarded to the Disclosing Party promptly thereafter. Prior to disclosing any Confidential Information to such person/s, the Receiving Party shall inform them of the confidential nature of the information and their obligation to refrain from disclosure of the Confidential Information. The Receiving party shall use at least the same degree of care in safeguarding the Confidential Information as it uses or would use in safeguarding its own Confidential Information and shall take all steps necessary to protect the Confidential Information from any unauthorized or inadvertent use. In no event shall the Receiving Party

take all reasonable measures that are lesser than the measures it uses for its own information of similar type. The Receiving Party and its Representatives will immediately notify the Disclosing Party of any use or disclosure of the Confidential Information that is not authorized by this Agreement. In particular, the Receiving Party will immediately give notice in writing to the Disclosing Party of any unauthorized use or disclosure of the Confidential Information and

The Receiving Party and its Representatives shall not disclose to any person including, without limitation any corporation, sovereign, partnership, company, Association of Persons, entity or individual

(i) the fact that any investigations, discussions or negotiations are taking place concerning the actual or potential business relationship between the parties,
(ii) that it has requested or received Confidential Information, or
(iii) any of the terms, conditions or any other fact about the actual or potential business relationship.

This confidentiality obligation shall not apply only to the extent that the Receiving Party can demonstrate that:

(a) the Confidential Information of the Disclosing Party is, or properly became, at the time of disclosure, part of the Public domain, by publication or otherwise, except by breach of the provisions of this Agreement; or

(b) was rightfully acquired by the Receiving Party or its Representatives prior to disclosure by the Disclosing Party;

(c) was independently developed by Receiving Party or its Representatives without reference to the Confidential Information; or

(d) the Confidential Information of the Disclosing Party is required to be disclosed by a Government agency, is the subject of a subpoena or other legal or demand for disclosure; provided, however, that the receiving party has given the disclosing party prompt written notice of such demand for disclosure and the receiving party reasonably cooperates with the disclosing party's efforts to secure an appropriate protective order prior to such disclosure.
(e) is disclosed with the prior consent of or was duly authorized in writing by the disclosing party.

3. RETURN OF THE MATERIALS

Upon the disclosing party's request, the receiving party shall either return to the disclosing party all Information or shall certify to the disclosing party that all media containing Information have been

destroyed. Provided, however, that an archival copy of the Information may be retained in the files of the receiving party's counsel, solely for the purpose of proving the contents of the Information.

4. OWNERSHIP OF CONFIDENTIAL INFORMATION

The Disclosing Party shall be deemed the owner of all Confidential Information disclosed by it or its agents to the Receiving Party hereunder, including without limitation all patents, copyright, trademark, service mark, trade secret and other proprietary rights and interests therein, and Receiving Party acknowledges and agrees that nothing contained in this Agreement shall be construed as granting any rights to the Receiving Party, by license or otherwise in or to any Confidential Information. Confidential Information is provided “as is” with all faults.

By disclosing Information or executing this Agreement, the disclosing party does not grant any license, explicitly or implicitly, under any trademark, patent, copyright, mask work protection right, trade secret or any other intellectual property right.

In no event shall the Disclosing Party be liable for the accuracy or completeness of the Confidential Information. THE DISCLOSING PARTY DISCLAIMS ALL WARRANTIES REGARDING THE INFORMATION, INCLUDING ALL WARRANTIES WITH RESPECT TO INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS AND ALL WARRANTIES AS TO THE ACCURACY OR UTILITY OF SUCH INFORMATION. Execution of this

Agreement and the disclosure of Information pursuant to this Agreement does not constitute or imply any commitment, promise, or inducement by either party to make any purchase or sale, or to enter into any additional agreement of any kind.

5. REMEDIES FOR BREACH OF CONFIDENTIALITY

(a) The Receiving Party agrees and acknowledges that Confidential Information is owned solely by the disclosing party (or its licensors) and that any unauthorized disclosure of any Confidential Information prohibited herein or any breach of the provisions herein may result in an irreparable harm and significant injury and damage to the Disclosing Party which may be difficult to ascertain and not be adequately compensable in terms of monetary damages. The Disclosing Party will have no adequate remedy at law thereof, and that the Disclosing Party may, in addition to all other remedies available to it at law or in equity, be entitled to obtain timely preliminary, temporary or permanent mandatory or restraining injunctions, orders or decrees as may be necessary to protect the Disclosing Party against, or on account of, any breach by the Receiving Party of the provisions contained herein, and the Receiving Party agrees to reimburse the reasonable legal fees and other costs incurred by Disclosing Party in enforcing the provisions of this Agreement apart from paying damages with interest at the market rate prevalent on the date of breach to the Disclosing Party.

(b) The Receiving Party agrees and acknowledges that any disclosure, misappropriation, conversion

or dishonest use of the said Confidential Information shall, in addition to the remedies mentioned above, make the Receiving Party criminally liable for Breach of Trust under section 405 of the Indian Penal Code.

6. TERM

This Agreement shall be effective on the first date written above and shall continue in full force and effect at all times thereafter. This Agreement shall however apply to Confidential Information disclosed by the Disclosing Party to the Receiving Party prior to, as well as after the effective date hereof. The Receiving Party acknowledges and agrees that the termination of any agreement and relationship with the Disclosing Party shall not in any way affect the obligations of the Receiving Party in not disclosing of Confidential Information of the Disclosing Party set forth herein. The obligation of non-disclosure of Confidential Information shall bind both parties, and also their successors, nominees and assignees, perpetually.

7. GOVERNING LAW & JURISDICTION

This Agreement shall be governed by and construed with solely in accordance with the laws of India in every particular, including formation and interpretation without regard to its conflicts of law By disclosing Information or executing this Agreement, the disclosing party does not grant any license, explicitly or implicitly, under any trademark, patent, copyright, mask work protection right, trade secret or any other intellectual property right.

In no event shall the Disclosing Party be liable for the accuracy or completeness of the Confidential Information. THE DISCLOSING PARTY DISCLAIMS ALL WARRANTIES REGARDING THE INFORMATION, INCLUDING ALL WARRANTIES WITH RESPECT TO INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS AND ALL WARRANTIES AS TO THE ACCURACY OR UTILITY OF SUCH INFORMATION. Execution of this Agreement and the disclosure of Information pursuant to this Agreement does not constitute or imply any commitment, promise, or inducement by either party to make any purchase or sale, or to enter into any additional agreement of any kind.

8. REMEDIES FOR BREACH OF CONFIDENTIALITY

(a) The Receiving Party agrees and acknowledges that Confidential Information is owned solely by the disclosing party (or its licensors) and that any unauthorized disclosure of any Confidential Information prohibited herein or any breach of the provisions herein may result in an irreparable harm and significant injury and damage to the Disclosing Party which may be difficult to ascertain and not be adequately compensable in terms of monetary damages. The Disclosing Party will have no adequate remedy at law thereof, and that the Disclosing Party may, in addition to all other remedies available to it at law or in equity, be entitled to obtain timely preliminary, temporary or permanent mandatory or restraining injunctions, orders or decrees as may be necessary to protect the Disclosing Party against, or on account of, any breach by the Receiving Party of the provisions

contained herein, and the Receiving Party agrees to reimburse the reasonable legal fees and other costs incurred by Disclosing Party in enforcing the provisions of this Agreement apart from paying damages with interest at the market rate prevalent on the date of breach to the Disclosing Party.

(b) The Receiving Party agrees and acknowledges that any disclosure, misappropriation, conversion or dishonest use of the said Confidential Information shall, in addition to the remedies mentioned above, make the Receiving Party criminally liable for Breach of Trust under section 405 of the Indian Penal Code.

9. TERM

This Agreement shall be effective on the first date written above and shall continue in full force and effect at all times thereafter. This Agreement shall however apply to Confidential Information disclosed by the Disclosing Party to the Receiving Party prior to, as well as after the effective date hereof. The Receiving Party acknowledges and agrees that the termination of any agreement and relationship with the Disclosing Party shall not in any way affect the obligations of the Receiving Party in not disclosing of Confidential Information of the Disclosing Party set forth herein. The obligation of non-disclosure of Confidential Information shall bind both parties, and also their successors, nominees and assignees, perpetually.

10. GOVERNING LAW & JURISDICTION

This Agreement shall be governed by and construed with solely in accordance with the laws of India in every particular, including formation and interpretation without regard to its conflicts of law

ANNEXURE 10 – MINIMUM FUNCTIONAL & TECHNICAL SPECIFICATIONS

[TO BE INCLUDED IN 'COVER – A' ELIGIBILITY CUM TECHNICAL BID ENVELOPE]

EDR/XDR Technical Specifications				
#	**EDR/XDR Technical Specifications**	**Compliance (Yes/No)**	**Evidence**	**Remarks (If Any)**
1	The solution must support endpoints/clients and should consist of following components 1.Endpoint Protection(EPP)-should be an On-prem solution for EPP component 2.Anti APT or sandboxing --should be On-prem for anti APT or sandboxing solution 3.EDR/XDR--should be Hybrid/On-prem solution with a broker server, The Hybrid component of solution should be hosted on Cloud based in India at DC and DR.			
2	The solution should be compatible with multiple operating systems like Windows, Linux, Mac, Android, IOS etc.			
3	The solution must not be declared End of life during contract period, and should have a roadmap for next 5 years In case OEM declares their product end of life during contract period ,bidder should provide upgraded version of product at no additional cost			
4	Policy must be able to define whitelists to implement exceptions to the base policy			
5	Solution must support high availability and disaster recovery functions			
6	Solution must have a deeply functional and documented API to support integration and automation across the various platforms			
7	Solution must have a central console for defining policy, creating groups of systems/users, logging, deploying updates, reporting			
8	The solution must have professional OEM support for 24x7x365 (on-call/Remote)			
9	Must provide role-based access to the console to allow specific admins to carry out read/write/read & write as per permission			
10	Ability to exclude files and folders from scans.			
11	Granular control of policy based on group/device/user			
12	The solution should only enable Admins to remotely run the PowerShell script on the client			
13	The solution must have support of importing and preventing custom IOCs.			
14	Console access should support using 3rd party systems authentication (Entra ID, Two Factor Authentication, etc.)			
15	The solution shall use a secure mechanism for registering a new client installation to the Solution.			
16	The solution must allow to manage the agent version and components from the management interface			
17	The solution should be able to provide real time email alerts			

18	The solution should be able to provide pre-defined and customized Reports as per requirement			
19	Solution should be configurable for minimal system resource utilization			
20	The solution allows upgrade to newer versions without performing a reboot			
21	The solution package size will include only the relevant components for deploying in a single installer			
22	When performing upgrades, the solution should download only the accumulated changes from the installed version			
23	Solution must continuously collect system events necessary for detection and analysis. Vendor must list specific items that are collected in real-time. Examples must include, but not limited to, process events, file & registry modifications, network connections, cross-process activity, command line arguments, windows events, DNS queries and responses			
24	Solution must continuously monitor and report findings as quickly as possible. If an endpoint cannot immediately report findings, results must be stored locally until they can be uploaded to the solution's central management system			
25	Solution must capture detailed metadata around binaries and processes that are executed on endpoints. Details must include, but not limited to, the binaries hash (MD5, SHA256, SHA-1, SHA-2), publisher information, code signing details, frequency observed in our environment, version information, and filesystem owner			
26	The solution should have the ability to customize user notifications			
27	The solution should have the ability to control the level of messages to show to users			
28	Solution must provide a way to isolate a system that ensures preventative controls are preserved through reboots			
29	Isolation settings must be pre-set to allow endpoint to be isolated from threats but able to connect to investigation/remediation systems.			
30	Solution must be able to immediately apply preventive controls (block specific activity or known malicious, etc.)			
31	The solution will Automatically learn and authorize logged in users			
32	The solution will enforce Firewall rules to allow or block network traffic to endpoint computers based on connection information, such as IP addresses, ports, and protocols			
33	The solution will be used to restrict or allow IPV4/6 network traffic			
34	The solution’s client Firewall should remain active during a client upgrade.			
35	Report to automatically identify the malicious activity entry point and highlight the potential damage, remediation action and the entire chain of attack.			
36	The solution will be used to restrict network access for specified applications. The Endpoint Security administrator defines policies and rules that allow, block or terminate applications and processes.			

37	The solution will be able to Whitelist\Blacklist applications.			
38	The solution will protect the computer from all kinds of malware threats, ranging from worms and Trojans to adware.			
39	The solution should have the feature to allow scheduled scanning and blocking of local drives Optical drives, Removable devices, storage of Mobile like mass storage, etc			
40	In case of a malware detection, the solution will be able to quarantine infected files.			
41	The solution will protect against existing and zero-day ransomware without requiring signature updates			
42	The solution will remediate and restore files that were encrypted during a ransomware attack.			
43	The solution will immediately prevent or detect on malicious behaviours regardless of if the machine is online or offline			
44	The solution will detect and prevent known and unknown fileless attacks			
45	The solution must be able to identify zero-days Malicious hashes even if they are not familiar with any reputation service			
46	The solution will identify and block out-going communication to malicious C&C sites			
47	The solution must have scrubbing capabilities with no added hardware. Incoming files will be extracted of all potential malicious content such as scripts, macros and active content			
48	When scrubbing, the original file must be accessible by end user if is found to be benign by the sandbox			
49	Incoming files will be emulated by sandboxing for potentially malicious content.			
50	The solution must block the user from browsing to a known and unknown malicious URLs or domains			
51	All files written on the filesystem will be monitored and statically analysed. If found as potentially malicious the files will be emulated by sandboxing and quarantined if found as malicious			
52	The solution must be able to completely clean the endpoint from any leftovers of the attack in the case the sandbox found the file to be malicious			
53	Solution will automatically create an incident analysis for every detection/prevention that occurs. This analysis should include process execution trees even across boots if relevant			
54	Forensic report will automatically identify the malicious activity entry point and highlight the potential damage, remediation action and the entire chain of attack.			
55	The solution will enhance third-party anti-malware or security detections by automatically building and visualizing an incident report			
56	The Forensics report will log, present and un-obfuscate PowerShell scripts used during an attack			

57	The solution will list reputation analysis on files, URLs and IPs used during an attack.			
58	The solution will be able to follow indirect methods of execution used by malware like WMI calls and Injections to be able to trace the activity of more advanced malware			
59	The solution must detect/identify the following: Remote Execution Service Creation Process Discovery Application Window Discover			
60	Solution will allow for the searching of multiple type of undetected sensor data including File, Process, Network, Registry, Injection and User data			
61	The solution will allow for remediation of any file or process found through the EDR platform			
62	The solution will allow for forensics analysis and report of any indicator found through the EDR platform.			
63	The solution will provide multiple manual remediation options, such as Quarantine, Kill Process and Forensics Analysis with remediation			
64	The solution will provide a central management ability to isolate machines remotely			
65	Solution will allow for searching incidents by Mitre Attack techniques.			
66	The solution must have the ability to view MAC addresses for every computer sending data.			
67	The solution should generate periodic reports on malware types, types of vulnerabilities exploited etc.			
68	The solution must have the ability to generate visual reports			
69	The solution should showcase affected process, affected registry keys & affected files in OS environment			
70	The solution will showcase malicious file emulation in Sandbox environment			
71	The solution must leverage behaviour-based detection and AI-ML powered analytics to identify and prevent known and unknown threats.			
72	Must aggregate and correlate security telemetry from endpoints, networks, cloud, and identity sources for comprehensive threat detection.			
73	Should reduce alert fatigue by intelligently grouping related alerts and prioritizing security incidents.			
74	Must provide machine-generated insights and guided investigations to enhance analyst efficiency.			
75	Should integrate with global threat intelligence sources to enhance detection and response capabilities.			
76	Must provide behavioural analytics and risk scores			

77	Must support both real-time and historical data searches for proactive threat hunting.			
78	Should offer predefined and customizable playbooks for rapid incident containment and mitigation.			
79	Must predict potential breaches and assess the effectiveness of existing security countermeasures.			
80	Must protect against file-based and fileless attacks using AI-driven analytics and behaviour-based detection.			
81	Should also enforce granular control over USB, Bluetooth or wireless endpoint device access based on security policies.			
82	Must provide host-based firewall protection to secure endpoint communications and data.			
83	Should perform AI-driven forensic analysis to determine attack origins and impact.			
84	Must correlate endpoint activity with network telemetry to improve threat detection accuracy.			
85	Should provide on premise threat analysis sandbox for detecting and analysing unknown malware and attack techniques.			
86	The endpoint agent must be lightweight and ensure minimal impact on system performance while enabling continuous monitoring.			
87	Must provide visibility into identity-based threats such as credential compromise and lateral movement.			
88	Should enable collection of volatile memory and endpoint telemetry for advanced threat investigations.			
89	Should provide an intuitive management console with graphical reports and customizable security insights, for the management.			
90	Must offer open APIs for integration with SIEM, SOAR, threat intelligence platforms, and other security solutions.			
91	Should enable one-click actions for isolating infected endpoints, terminating malicious processes, and restricting network activity.			
92	Must provide security visibility and enforcement across on-premises, private cloud, and public cloud environments.			
93	Should integrate with security orchestration tools to automate incident response workflows.			
94	The unified endpoint agent must provide dedicated modules for Next-Gen AV, EDR, device control, rogue device detection, firewall, vulnerability detection, FIM, remote response, all accessible through a single console without relying on custom behaviour rules.			
95	The unified endpoint agent must be a standalone package from the same OEM, containing all required components without reliance on third-party or customer solutions. It must be identical across all systems, with all features integrated into a single agent.			
96	The endpoint agent must have tamper protection to prevent alteration, termination, or removal of its files, processes, and data, even by administrators. Uninstallation or disabling must require an authorization token or key.			

97	The solution must allow whitelisting of authorized removable devices from the same console, with options for read-only or read/write access, based on device type, serial number, vendor, and product name.			
98	The agent must monitor and classify outgoing data transfers to USB devices, scanning for malware and reporting details on the console, including endpoint, user, device, transfer summary, and timestamp, with a policy-controlled enable/disable option.			
99	Provide a solution that identifies vulnerabilities tied to assets without deploying additional agents.			
100	Ensure real-time vulnerability status for all Windows endpoints without requiring a scan.			
101	Deliver detailed insights for each vulnerability, including severity, vulnerable products, attack vector, number of affected hosts, and patch recommendations.			
102	Enable automatic closure of vulnerabilities upon patch installation without requiring user intervention.			
103	Detect and highlight unpatched vulnerabilities that are actively targeted.			
104	Offer comprehensive vulnerability management, not just reporting.			
105	Prioritize unpatched vulnerabilities on systems generating detections.			
106	Provide visibility into whether a system reboot is required after patch installation.			
107	The solution must proactively detect attacks that evade platform detections.			
108	The solution must facilitate a customer portal for submitting suspicious file samples, reporting technical issues, and tracking the progress of submitted requests.			
109	Solution should continuously monitor browser activity for malicious behaviour, such as suspicious websites, malicious extensions, or phishing attempts			
110	Solution should detect and mitigate unique vulnerabilities of web browsers and the types of threats that target them			
111	Solution must offer Safe Browsing by protecting critical functions in web browsers to neutralize the threat, such as blocking malicious websites, quarantining malicious extensions, or alerting users to potential risks			
112	Solution must mitigate exploits in vulnerable applications a) Protect web browsers b) Protect web browser plugins c) Protect Java applications d) Protect media applications			
113	Solution should provide protection against * Prevent Ransom attacks that target MBR. * Destructive Boot records attacks. * Prevent boot kit installation.			

114	Solution should support Malicious Traffic Detection (MTD)			
115	Solution must support Runtime Behaviour Analysis / HIPS			

DLP Technical Specifications				
#	**DLP Technical Specifications**	**Compliance (Yes/No)**	**Evidence**	**Remarks (If Any)**
1	The solution should be a On-premises based offering and bidder should factor in the required underlying hardware			
2	The solution should be compatible with multiple operating systems like Windows, Linux, Mac, Android, IOS etc.			
3	The solution must not be declared End of life during contract period, and should have a roadmap for next 5 years In case OEM declares their product end of life during contract period ,bidder should provide upgraded version of product at no additional cost			
4	Solution must support high availability and disaster recovery functions			
5	Solution must have a deeply functional and documented API to support integration and automation across the platform available with the customer			
6	Solution must have a central console for defining policy, creating groups of systems/users, logging, deploying updates, reporting			
7	The solution must have OEM support 24x7x365.			
8	Must provide role-based access to the console to allow specific admins to carry out read/write/read & write as per permission			
9	Granular control of policy based on group/device/user.			
10	The solution should have compatibility of Scale-out when needed.			
11	The solution should be able to provide a remote collection of troubleshooting logs			
12	Solution must support DPDP, IRDAI, RBI guidelines			
13	Console access should support using 3rd party systems authentication (Two Factor Authentication)			
14	Solution must use provide modern and easy remote deployment/installation/uninstallation methods (Including script support)			
15	The solution must allow to manage the agent version and components from the management interface			
16	The solution should be able to provide real-time email alerts			
17	The solution should be able to provide pre-defined and customized Reports as per requirement for Audit and internal reporting purpose			
18	Solution is configurable for minimal system resource utilization			
19	The solution allows upgrade to newer versions without performing a reboot.			
20	The solution should have the capability of OCR techniques.			
21	The solution should have the capability of Anomaly detection and predictive analytics.			

22	The solution should have the capability of Threat intelligence and User behaviour analytics.			
23	The solution should have the capability of automation and incident response.			
24	The solution should have the capability of protecting sensitive data while taking print screens/screenshots.			
25	The solution should have the capability of putting protective measures while sending sensitive information via Bluetooth			
26	The solution should have the capability of Intelligent data discovery by using AI techniques.			
27	The solution must be able to capture data leakage over image files, zip files, etc.			
28	The solution should have the capability of encrypting the data transferring over cloud based storage solutions. It Should support both Native and Portable Encryption and manage the removable media Encryption and DLP policies from the same management Console.			
29	The solution should have the capability of creating policies by using Classifiers, File types, File size, Regular Expressions, Classified data, fingerprinted data etc.			
30	It should also have the capability to support Email DLP in Microsoft Azure, AWS, GCP etc CSPs for Office 365/Exchange in the future, ensuring a seamless upgrade process. Additionally, management for Endpoint, Email, and Web DLP should be centralized and unified within the same management platform.			
31	The DLP solution ensures compatibility with existing endpoints			
32	Solution must continuously collect system events necessary for detection and analysis. Vendor must list specific items that are collected in real time			
33	Solution must continuously monitor and report findings as quickly as possible. If an endpoint cannot immediately report findings, results must be stored locally until they can be uploaded to the solution's central management system			
34	Solution must allow for real-time alerting or logging of notable events based on custom content (behaviours) or atomic indicators of compromise based on data types identified.			
35	Solution must capture detailed metadata around binaries and processes that are executed on endpoints.			
36	The solution should be able to alert and notify sender and the policy owner whenever there is a policy violation, Different notification templates for different audience should be possible. Solution must support Incident Management REST APIs on historical actions performed on incidents, such as “Change Status” or comments added by admins.			
37	The solution should have the ability to control the level of messages to show to users			
38	Solution must be able to immediately apply preventive controls (block specific activity)			

39	Solution must allow analysts the ability to quickly pivot between different activities observed on an endpoint and provide contextual information if available			
40	The solution should have more than 50 pre-defined applications and multiple application groups and allow each application/application group to monitor operations like Cut/Copy, Paste, File Access and Screen Capture or Download. Also solution should have the capability to define the third party application.			
41	The solution should be able to define the policies for the inside and out of office endpoint machines. The endpoint solution should be able to perform discovery only when the endpoint is connected to external power or Machine is Idle.			
42	The endpoint solution should have capabilities to monitor applications and ensure unauthorized applications do not have access to sensitive files.			
43	The solution will be able to Whitelist\Blacklist applications.			
44	The solution will allow scheduled scanning of local drives and Network locations			
45	The solution should be able to capture data leakage if the client is offline and doesn't have an internet connection			
46	The solution will leverage AI/ML and behaviour analytics to identify data leakage and apply preventive Controls.			
47	The solution will identify and block out-going communication over Email, web, and External Media.			
48	Solution will automatically create an incident analysis for every detection/prevention that occurs.			
49	Employ different fingerprinting methods to signify sensitive data.			
50	Capability to exert sufficient control on external devices being connected in the environment.			
51	Flexible reporting options for technical as well as high level reports.			
52	The solution should have the ability to automatically protect documents at central cloud based file servers i.e. Files should get automatically protected based on its classification or content.			
53	The solution should have the ability to automatically protect documents at the endpoint with DRM policies by integrating with DLP systems i.e. Files should get automatically protected based on its classification or content. Document/File, at any stage, must not travel outside the endpoint (user laptop or desktop) for protection.			
54	The solution should be able to monitor data copied to network file shares and should enforce structured and unstructured fingerprint policies even when disconnected from corporate network.			
55	The endpoint would be able to store both structured and unstructured fingerprints on the endpoint itself and should perform all analysis locally and not contact and network components to reduce WAN overheads.			

56	The solution should Provide “Cloud Storage Applications” group which monitor sensitive content accessed by these cloud storage application on the endpoint and prevent sensitive data from uploading to the cloud. For Example (Should support from day 1(Windows 11, 10) -Amazon Cloud Drive, Box, Dropbox, Google Drive, SkyDrive, iCloud.			
57	The Endpoint DLP Solution must be able to encrypt data when business classified data is sent to removable media drives. The encryption solution should be inbuilt with DLP component and not dependent upon any 3rd party solution to meet the requirement. Solution should provide certified installation of the 3rd party clouds like AWS, Azure and GPC.			
58	The solution should support the multiple Endpoint Profile Creation for the Better Security between the different departments. Encryption Keys are also should be isolated between the different departments. The endpoint installed should have the capability to create the Bypass ID after validation by the administrator by generating the Passcode.			
59	The solution should have a comprehensive list of pre-defined policies and templates with over 1700+ patterns to identify and classify information.			
60	The solution should be able to do full binary fingerprint of files and also should be able to detect even if partial information gets leaks from fingerprinted files or folders			
61	The solution should be able to recursively inspect the content of compressed archives. Solution must also support disable/enable of policies so easy of management.			
62	The solution should enforce policies to detect low and slow data leaks			
63	The solution should be able to identify data leaked in the form unknown and known encrypted format like password protected word document			
64	The solution should be able to identify and block malicious activity like data thefts through files encrypted using non-standard algorithms.			
65	The proposed DLP Solution must be able to detect Data Classification Labels applied by Data Classification partners by reading metadata as well as custom header analysis. Solution must support Rest API for policy management along import and export of policies as well.			
66	The solution should support the templates for detecting the Deep Web Urls- .i2P and .Onion , Encrypted attachments to competitors , Password Dissemination , User Traffic over time , Unknown Encrypted File Formats Detection. The solution should support detection of PKCS #12 files (.p12, .pfx) that are commonly used to bundle a private key with its X.509 certificate.			
67	Monitor any suspicious attachment embedded with the email.			

68	The incident should include a clear indication of how the transmission or file violated policy (not just which policy was violated), including clear identification of which content triggered the match and should allow opening of original attachment directly from the management UI			
69	The incident should display the complete identity of the sender(Full name, Business unit, manager name etc.) and destination of transmission for all endpoint channels. The solution should also allow assigning of incidents to a specific incident manager			
70	The solution should provide automatic notification to incident managers when a new incident is assigned to them and the incident should not allowed for deletion even by the product administrator			
71	The solution should allow a specific incident manager to manage incidents of specific policy violation, specific user groups etc.			
72	The system should control incident access based on role and policy violated. The system should also allow a role creation for not having rights to view the identify of the user and the forensics of the incident. RBAC should provide the functionality to hide source and destination information from the admins and solution must support bypassing the endpoint with ability to still monitor the user.			
73	The system should have options to create a role to see summary reports, trend reports and high-level metrics without the ability to see individual incidents			
74	The system should allow incident managers and administrators to use their Active directory credentials to login into the console. Solution must segregate roles and responsibilities into users that can modify policies & rules, users that can only view policies & rules and users that are restricted from viewing policies & roles.			
75	The solution should have a dashboard view designed for use by executives that can combine information from data in motion (network), data at rest (storage), and data at the endpoint (endpoint) in a single view along with Single management for managing policies for DLP channels like endpoint, Web, Email and removable media encryption. DLP and Data Classification should have single OEM support			
76	The system should allow reports to be mailed directly from the UI and should allow automatic schedule of reports to identified recipients			
77	The reports should be exported to at least CSV, PDF formats			
78	The system should provide options to save specific reports as favourites for reuse			
79	The system should have lots of pre-defined reports which administrators can leverage			
80	The DLP Solution must provide visibility into Broken Business process. For ex:-if unsecured sensitive content is sent daily from several users to a business partner, the users are probably not aware that they are doing something wrong. Solution must support APIs for Policy management that can be used to manage DLP and Discovery policies, rules and resources along with APIs for Incident			

	Management to get a list of DLP & Discovery incidents, update & remediate those incidents.			
81	The Proposed DLP engine must performs a post-processing incident grouping step to avoid displaying related incidents in different cases. All incidents from the same user that have the same classification are combined into a group and DLP case card.			
82	The DLP solution should support as an API be able to provide the risk adaptive based protection by dynamically calling the action plan based on the Risk in future if required.			
83	The system should allow automatic movement or relocation of file, delete files during discovery over cloud based storage			
84	The system should display the original file location and policy match details for files found to violate policy			
85	The system should leave the "last accessed" attribute of scanned files unchanged so as not to disrupt enterprise backup processes			
86	The system should support incremental scanning during discovery to reduce volumes of data to be scanned.			
87	The OEM should have own technical support center in India.			
88	The solution should detect and prevent content getting posted or uploaded to specific websites, blogs, and forums accessed over HTTP, HTTPS. The solution should be able to monitor FTP traffic including fully correlating transferred control information and should be able to monitor IM traffic even if its tunnelled over HTTP protocol.			
89	The proposed solution work as a MTA to receive mails from mail server and inspect content before delivering mails to next hop and should quarantine emails that are in violation of company policy.			
90	The solution should support Email DLP in HCL Domino for all users. All licenses required for the same should be included and management should be from the same centralized management platform			
91	The proposed solution should provide Incident Workflow capabilities where user/Business Manager can remediate the DLP policy violations actions from handsets/emails without logging into the Management Console			
92	The DLP dashboard must display the number of cases in the designated period that fall above the risk score threshold that you've selected. Risk score thresholds must be customizable and instantly produce an report to prioritize the cases from high-to-low risk levels by leveraging analytics or machine learning technologies. Solution must support Rest API for policy management along import and export of policies as well			
93	Endpoint must support the following operations on sensitive data that your DLP endpoint can address:			

94	Copy and paste controls (i.e., clipboard activities)			
95	Save content to different locations, including saving to:			
96	Local folders			
97	Remote file shares			
98	Saving to cloud storage locations			
99	Ability to seamlessly integrate with encryption and selectively encrypt data on the basis of designed policies			
100	Enforce compliance over data sitting in different locations and be able to remediate all the issues identified for ensuring compliance.			
101	Ability to handle data being written on different types of media and option to monitor or prevent the same			
102	Capability to monitor and block all the traffic flowing out of the network, irrespective of Policies being in place or not			
103	Quick Deployment capability and Single Management Console for configuring Uniform Policies			
104	The solution must detect/identify and block the following:			
105	Password protected file			
106	Encrypted file			
107	Sensitive data sent over mail			
108	Sensitive data uploaded over the web			
109	Sensitive data copied to External storage (USB, HDD, Mobile Transfer)			
110	Sensitive data while taking printouts			
111	The solution must have the ability to generate visual reports Solution must provide an agent and DLP Component's health status.			
112	The DLP solution should be able to go beyond known policies and provide Forensic capability on all historic data. Thus, the DLP should safeguard and ensure compliance by protecting sensitive data wherever it lives—on the network or in storage systems, while saving time and money with centralized deployment, management, and reporting.			
113	The solution must have Integration with SIEM and other security solutions (DRM, Data classification, CASB, PIM/PAM,ITSM, AD/LDAP etc.)			
114	Solution must support data at rest scanning for Databases, SharePoint and File systems			
115	Solution must support SMB, NFS and CIFS for Windows and non-Windows based file shares			
116	Solution must support TCP or ICMP scan methods when searching network shares			
117	Network Data discovery tasks must have a scheduler option by: once, daily, weekly or continuously			

118	Network Data discovery task must support inclusion and exclusion by file type, folders, age or size			
119	Network Data discovery task must support differential and full scanning options. The system should support incremental scanning during discovery to reduce volumes of data to be scanned.			
120	Network Data discovery must have an option to preserve original access time			
121	Network Data discovery must support bandwidth allocation for discovery process scanning			
122	Proposed solution should be able to deploy agent using common software methods like GPO, SCCM, etc. Proposed solution should support integration with SaaS based Active Directory, LDAP solutions			
123	Solution should allows definition of what applications are trusted/ untrusted and granting them their associated rights and support granular application control for DLP , for example solution should have inbuilt application groups and application lists where data cannot be copied / pasted , accessed etc.			
124	Solution should allow dynamic, real-time tuning of rules and policies & should provide hierarchical management of rules, including higher-level groupings that map to business objectives			
125	Solution should provide emergency offline based override of policies based of administrative password and is the same recorded for the activities			
126	Solution should allow powerful rule construction, using keywords and/or regular expressions in standard Boolean logic			
127	The Bidder to ensure that OEM should provide Customer Advocates for better case management & should serve as the primary point of contact during escalation and Customer Advocate should do annual value review to evaluate real progress in achieving information security goals of the organisation.			
128	The solution must provide an option to allow data owners to send their own personal data (e.g., personal credit card numbers) outside the corporate network without violating fingerprint rules.			
129	The solution must detect unstructured documents of a specified type (e.g., proprietary source code, legal contracts, insurance claims) using native machine-learning capabilities to analyse a small sample set, without requiring fingerprints while maintaining accuracy comparable to fingerprinting.			
130	The solution must utilize a lightweight index of document features deployable across all products in the suite, ensuring the endpoint agent remains compact and resource-efficient, and must also detect new or never-before-seen documents of the specified type.			
131	The solution must integrate directly with Active Directory (AD) to create user- or group-based sender, recipient, and endpoint detection rules, allowing different policies to be applied based on the logged-in user, even on shared machines.			

132	The solution must monitor and block confidential data use across all applications, including unauthorized encryption programs, with built-in support for Skype, Webex, LiveMeeting, Office Communicator, Bluetooth, iTunes, and Google Talk.			
133	The solution must enforce metadata-based policies, block print screen actions, and cover Citrix-published apps and virtual desktops using agents on Citrix server hosts only.			
134	The solution must ensure agent tamper-proofing, hiding it from system interfaces, encrypting communications, and requiring a password for uninstallation.			
Data Classification & Discovery Technical Specifications				
#	**Data Classification**	**Compliance (Yes/No)**	**Evidence**	**Remarks (If Any)**
1	The solution must deploy in On-prem.			
2	The solution must have OEM support 24x7x365.			
3	The solution should be in High Availability at primary site and DR site			
4	The solution should be able to switch to DR seamlessly			
5	The solution should provide high availability seamless DC-DR migrations and vice- versa			
6	The solution should support scalability to meet future requirements			
7	The solution should enable the classification and should support all mainstream server, desktop ,mobile, tablet and laptop Operating Systems			
8	The solution should have the capability to integrate with third party Data Leak Prevention solutions and Data/Information Rights Management Solutions that are available in the market. Details to be given			
9	The solution should have the capability to integrate with exsiting security technologies such as AD, PAM/PIM, SIEM, etc.			
10	The Solution should provide classification logs inside the classified file and at the centralized repository.			
11	The solution should be able to classify unstructured data, namely word/excel/PowerPoint/pdf documents and HCL Domino			
12	The Solution should Support for Email Servers like HCL Domino			
13	The solution should enable the classification of Word, Excel and PowerPoint documents from within Microsoft Office.			
14	The solution should apply meta data tagging for various file formats like document, excel, ppt, pdf, image files, text files etc.			
15	The solution shall have capability to send emails from mobile with classification applied for both IOS and Android based mobiles.			
16	The solution should be capable of integrating with OpenOffice to classify documents being created with OpenOffice.			
17	The solution should enable user can define different Classification labels like public, internal, confidential, restricted etc.			

18	The solution should be able to label the documents in Headers/Footers with a preselection capability for either header or footer or both.			
19	The solutions should be able to insert metadata tags in the documents and emails which can be read by DLP Solutions.			
20	The solution should be able to track initial classification and reclassification events at both document and central logging level.			
21	The solution should have the ability to classify based on context based on file attributes, ip, hostname, username etc. for example if finance team is creating a file with "shareholder_data" it should be classified as confidential.			
22	The solution should be able to blacklist domains for blocking emails originating out of Microsoft Outlook and also bind certain classification categories with a fixed domain name.			
23	The solution should trigger classification for document on Save, Save As, Print etc. and should be configurable using a management mechanism.			
24	The solution should trigger classification based on send, reply, forward emails.			
25	The solution should provide automated, suggestive and manual classification capability			
26	The solution shall have capability to classify multiple documents in one go.			
27	The solution shall ensure the enforcement of classification and should not allow user to bypass classification option in the said documents types using MS Office, OpenOffice and MS Outlook, pdf			
28	The solution should have capability to detect differential classification between an email and it's attachments and block the email from being sent			
29	The solution should detect unclassified documents attached in an email and block the user from sending the email.			
30	The solutions should not restrict the number of classification levels required to be created.			
31	The solution should have some guidance mechanism while user selects a classification level, to inform the users what is the context of a said classification level as per organization's policy			
32	The solution should be capable to deploy and enforcing user based policies.			
33	The solution should be able to identify information like Aadhar, Passport numbers, credit card ,insurance policy nformation for automated classification thru either inbuilt capability or should have capability to define regular expressions.			
34	The solution should be able to detect keywords as defined by the organization and enforce classification			
35	The solution should further allow policies which are based on a combination of keywords and regular expressions.			
36	The solution should allow administrators to define own regex for adding capability to detect any new type of regex.			

37	The solution should suggest a classification based in content, but should allow user to change the classification if required by taking a justification for the same and recording it in logs.			
38	The solution should Apply Rights Management on an outgoing email. Once classification is applied to the email it needs to be secured and only authorized users to get access to the email.			
39	The solution should log user activity while users are handling email, documents, and files.			
40	The solution should provide context-sensitive help throughout the user interface to support security training and help users select the correct classification and policy remediation options.			
41	The solution should have Manual, Automated and Suggested Classification feature			
42	User can define different Classification labels like public, internal, confidential, restricted etc.			
43	User should be able to set default classification labels for each department			
44	Ability to classify based on content like if Credit card or Aadhaar card is identified, tool should automatically classify file as restricted			
45	Ability to classify based on context based on file attributes, ip, hostname, username etc. for example if finance team is creating a file with "shareholder_data" it should be classified as confidential.			
46	Ability to customize visual marking, header, footer of word, excel, ppt etc.			
47	The solution should have Policy Configuration based on Departments and user groups from AD.			
48	The solution should have Print Protection: - Prevent user from printing sensitive files and emails.			
49	The solution should have Domain Policy: - User can provide the domain list and block sending emails with restricted content and attachment outside of the domain.			
50	The solution should have ability for Auto classification files whenever user will download based on content or context			
51	The solution should have Ability to set the classification labels based on occurrence of PII data like if a file contains only 1 policy number number it can be marked as confidential for business purpose while more than 5 it should be marked as restricted			
52	The solution should have Ability to prevent user from sending attachment without classifying			
53	The solution should have Ability to automatically detect PII types in email body attachment and subject based on classification policy			
54	The solution should have Ability to prevent user from sending attachment with confidential or restricted content to outside domain based on policy			
55	The solution should have Auto classification based on user roles like if Mail is sent from specific dept/mail id then it should be classified as Confidential.			

56	The solution should have ability User will be warned if they are trying to send any sensitive data over mail. They need to provide justification before sending. These events will be logged and triggered over mail based on requirement.			
57	The solution should Provide default classification department wise like if anyone from HR team has sent mail mark as internal for HR purpose.			
58	The solution should have Ability to prevent user from downgrading the classification labels for certain department and users like finance head can downgrade , but finance ops can not.			
59	The solution should support hierarchical and conditional classification fields, so that the appearance of a sub-field is conditional on the value selected in the higher-level field. For example, when a user selects “Restricted,” a sub-field is presented with a list of departments including “Office use”, “Branch use”, “P&IR” etc.			
60	The solution should support icon overlays to identify the classification of files in File Explorer.			
61	The solution should provide tooltips, classification descriptions, and help page links to assist users with classification policy.			
62	The solution should support the creation of unlimited custom metadata for interoperability (Department, PII type, Document category, PII count etc.), including custom X-headers.			
63	The solution should support customizable visual markings in email and documents (e.g. font (name/size/features), size, colour, and content).			
64	The solution should support the ability to quarantine files stored inappropriately, flag files for follow-up, or take action based on results of the scan. This may include quarantine, delete, encrypt through 3rd party encryption tools, etc.			
65	The solution should provide the ability to attach metadata to information objects, which can be leveraged by DLP solutions.			
66	The solution should provide the ability to write tags which can be read by DLP solution			
67	The Solution should be managed via a centralized management console.The solution should have capability to manage the complete solution from a central web console			
68	The Management console should have role based access and should integrate with Active directory / Privilege Access Management system for login access			
69	The solution should provide built-in reports and dashboards to analyse user behaviour and system health.			
70	The solution should provide a pre-built starter set of reports for the reporting database (in Excel) and Views and documentation to enable customers to write their own reports.			
71	The solution should provide a built-in dashboard for reviewing data classification scanning results for user activity, deployment.			

72	The solution should provide role based access for administrators, compliance teams where anyone other than administrators may not have access to full console.			
73	The solution should provide Customizable dashboard to create multiple dashboards based on user requirements.			
74	The solution should provide Dashboard to provide classification alerts based on timeframe			
75	The solution should provide Dashboard to identify which events triggered the classification policy warning like if user is sending a restricted document over mail , trying to print restricted document etc.			
76	The solution should be capable for centralized deployment of the solution components on all network systems and it should be capable to get machine inventory from AD to perform deployment.			
77	The solution should provide Easy deployment of agents with support of Active Directory			
78	The solution should have a capability to deploy, upgrade, uninstall the component without the use of any 3rd party software			
79	The solution should provideMinimal impact for end points . User should be able to choose low, medium and high usage for agents			
80	The solution should provide Auto update features for agents. User should be able to push the agents automatically after every release.			
81	The solution should be able to send policy and further changes to the clients without any need or intervention of a 3rd party software.			
82	The solution should have capability to deploy policies basis users, machines, groups etc.			
83	The unavailability of a management component/ server in no way shall impact the functioning of a client			
84	The solution should cache configurations locally for offline use.			
85	The solution shall deploy the client in the background and shall have no interface with the end user on whose PC the solution is being deployed. Same shall be applicable for upgrades, updates and uninstallation.			
86	Ability to move systems from one group to other			
87	Ability to see the managed/unmanaged status of each system			
88	Ability to see last communication date and time of system with the Management server.			
89	The solution should have Password vaults for to authenticate different targets so that admin does not have to enter passwords multiple time for agent less scans and database scans			
90	The solution should have Auto Pause and Resume option. Scan can be automatically paused or resume every day based on peak hours where more loads are in servers.			
91	The solution should have Ability to add targets based on IP and hostname for dynamic environment			

92	The solution should have Support various PII types like Aadhaars card, Pan Card, Driving license, National ID of different countries ,Policy numbers			
93	The solution should have Support for multiple privacy regulations like DPDPA			
94	The solution should have Ability to tag files for for classification for agent based and agent less discovery			
95	The solution should have AI/ML capability to reduce false positives			
96	The solution should have Pre trained AI models to identify images with Aadhaars Numbers, Credit cards , PAN Card, Password, Driving licenses of different states.			
97	The solution should haveScheduling automated scans with out user intervention - daily, weekly, monthly, quarterly etc			
98	The solution should have Full scan , Incremental scan and specific date scan. Only those file will be scanned which are modified after previous scan, if user will chooses incremental scan. This will help to reduce the time to discover sensitive data in subsequent scans.			
99	The solution should have Ability to identify sensitive data in data bases - which tables , which columns contains sensitive data			
100	The solution should have Ability to view the actual file data or table from the centralized console to validate the results easily			
101	The solution must have the capability to Discover, Classify and Protect the documents and emails without any user intervention			
102	The solution must have ability to assign classification level to discovered data elements according to policy			
103	The solution should be equipped with the ability to analyze and discover sensitive data, aligning with internal compliance requirements such as PII, PCI-DSS, and IRDAI classification.			
104	The solution must have the capability to do analysis(discovering sensitive data)Based on file types (MS-office, pdf's, TXT files,XML,HTML,JPEG,Compressed file's etc.)			
105	The solution must have the capability to do analysis(discovering sensitive data) along with host details.			
106	The solution must have the capability to do analysis(discovering sensitive data) based on Current Classification Level and to suggest classification.			
107	The solution must have the capability to Delete the sensitive data as a Remediation action if required.			
108	The solution must have the capability to move the sensitive data as a Remediation action if required.			
109	The solution must have the capability to replace the sensitive data as a Remediation action if required.			
110	The Solution should be managed via a centralized management console.The solution should have capability to manage the complete solution from a central web console			

111	The Management console should have role based access and should integrate with Active directory / Privilege Access Management system for login access			
112	The solution should provide built-in reports and dashboards to analyse user behaviour and system health.			
113	The solution should provide a pre-built starter set of reports for the reporting database (in Excel) and Views and documentation to enable customers to write their own reports.			
114	The solution should provide a built-in dashboard for reviewing data classification scanning results for user activity, deployment.			
115	The solution should provide role based access for administrators, compliance teams where anyone other than administrators may not have access to full console.			
116	The solution should provide Customizable dashboard to create multiple dashboards based on user requirements.			
117	The solution should provide Dashboard to provide discovery overview like how many targets completed scans every quarter vs not completed, Remediation taken etc.			
118	The solution should provide Dashboard to provide classification alerts based on timeframe			
119	The solution should provide Dashboard to identify which events triggered the classification policy. Solution must provide restrictions based on the sensitivity and classification of the data. If any unauthorized attempts occur then there must be a incident with the audit logs details.			
120	The solution should incorporate a Dashboard feature that allows for the identification of events that have triggered classification policy warnings. For example, it should be able to pinpoint instances such as when a user attempts to send a restricted document via email or tries to print a restricted document			
121	The solution should be capable for centralized deployment of the solution components on all network systems and it should be capable to get machine inventory from AD to perform deployment.			
122	The solution should provide Easy deployment of agents with support of Active Directory			
123	The solution should have a capability to deploy, upgrade, uninstall the component without the use of any 3rd party software			
124	The solution should provideMinimal impact for end points . User should be able to choose low, medium and high usage for agents			
125	The solution should provide Auto update features for agents. User should be able to push the agents automatically after every release.			
126	The solution should be able to send policy and further changes to the clients without any need or intervention of a 3rd party software.			
127	The solution should have capability to deploy policies basis users, machines, groups etc.			
128	The unavailability of a management component/ server in no way shall impact the functioning of a client			

129	The solution should cache configurations locally for offline use.			
130	The solution shall deploy the client in the background and shall have no interface with the end user on whose PC the solution is being deployed. Same shall be applicable for upgrades, updates and uninstallation.			
S. No	**Data Discovery**	**Compliance (Yes/No)**	**Evidence**	**Remarks (If Any)**
1	The solution should support the discovery and identification of large volumes of data, stored both on-premise and in the cloud. This includes the scanning of network file shares, SharePoint (on-premise and Online), as well as cloud storage providers.			
2	The solution should provide the ability to run scheduled scans to automatically classify files based on several factors, including the file properties/attributes, content, and/or metadata.			
3	The solution should support the ability to collect file information during scans, including file properties, classification (pre- and post-scan), and access controls. This data inventory identifies what the data is, where it is, and who has access to it.			
4	The solution should be able to automatically quarantine sensitive files from insecure storage folders to secure folders natively.			
5	The solution should natively be able to add retention date as metadata in documents, with values populated based on content, creation date, or modification date in the file.			
6	The solution should enable administrators to define policies with or without classification as part of the policy.			
7	The solution must support agent-based and agentless discovery mechanisms, allowing flexibility for different endpoint types (servers, desktops, virtual machines, etc.).			
8	The solution should support multi-format data scanning, including structured (databases), semi-structured (JSON, XML), and unstructured formats (PDF, DOCX, TXT, etc.).			
9	The solution should integrate with Data Loss Prevention (DLP) tools to extend enforcement based on classification results.			
10	The solution must support integration with cloud-native APIs for platforms such as AWS (S3, RDS), Azure (Blob, SQL), and Google Cloud (GCS, BigQuery) for deep and scalable data discovery.			
11	The solution should support optical character recognition (OCR) to discover sensitive data within image-based files (e.g., scanned documents, PDFs).			
12	The solution must enable custom classification rules, including regular expressions, keyword dictionaries, and context-based logic (e.g., proximity, pattern matching).			
13	The solution should support real-time discovery and classification for newly created or modified files via event-based monitoring.			
14	The solution should support data lineage tracking, showing the movement and transformation of sensitive data over time.			

15	The solution must provide a centralized dashboard for viewing discovered data across environments, along with filters for classification type, location, ownership, and risk score.			
16	The solution should include role-based access controls (RBAC) to ensure that only authorized personnel can access sensitive discovery results or configure scan rules.			
17	The solution should support automated remediation actions (e.g., quarantine, deletion, alert generation, ticket creation) based on policy violations.			
18	The solution should provide reporting and audit logs that are exportable and compliant with regulations such as GDPR, HIPAA, CCPA, and PCI-DSS.			
19	The solution must support multi-tenancy to enable logical separation of discovery results by business unit, department, or customer (in MSSP environments).			
20	The solution should provide data ownership attribution, identifying the user or group responsible for each file, based on file metadata or access patterns.			
21	The solution should support integration with IAM/IGA solutions to cross-check data access rights with user roles and entitlements.			
22	The solution should support data risk scoring based on sensitivity, exposure, and usage patterns, allowing prioritization of remediation efforts.			
23	The solution must be able to scan compressed archives (.zip, .rar, .7z) and nested folder structures to locate hidden sensitive data.			
24	The solution should support data discovery across email platforms such as HCL Domino			
25	The solution must be able to identify and classify personally identifiable information (PII), payment card information (PCI), protected health information (PHI), and intellectual property (IP).			
26	The solution should provide APIs or SDKs for integration with third-party tools and for custom workflows or dashboard creation.			
Patch Management Technical Specifications				
Sr No	**Patch Management Technical Specifications**	**Compliance (Yes/No)**	**Evidence**	**Remarks (If Any)**
	Operating System Management Support			
1	Windows Desktop OS			
2	Windows Server OS			
3	Linux OS			
	Windows Desktop OS (Agent Based Protocol)			
	Update and Driver management			
1	Configure Update Sync Interval			
2	Sync Driver Updates			
3	Configure Update Schedule			
	1. Update should Deploy upon approval			
	2. Update should deploy upon schedule			

	a) Update Time			
	b) Update Day			
	c) Update Week			
4	Force Reboot Devices after Updates			
5	Configure custom message before reboot			
6	Configure Retry failed updates			
7	Configure the number of times an update should be retried in case of failure			
	OS Upgrade Management			
1	Define the OS version for deployment			
2	Disable Windows Automatic Update during Upgrade			
3	Configure Update Schedule			
	1. Update should Deploy upon approval			
	2. Update should deploy upon schedule			
	a) Update Time			
	b) Update Day			
	c) Update Week			
4	Enable alert and deferral settings			
5	Allow users to provide alternate time for upto two times for installation or perform silent install when possible			
6	Prompt users to install the upgrade			
7	Configure Retry failed OS upgrade			
8	Configure the number of times an OS Upgrade should be retried in case of failure			
	Windows Desktop OS (Windows Based Protocol)			
1	Configure Auto Update Setting			
	1. Active Hours Start			
	2. Active Hours End			
	3. Active Hours Max Range			
	4. Manage automatic update behavior			
	a) Notify the user before downloading the Update			
	b) Auto install the update and then notify the user to schedule a device restart			
	c) Auto install and restart			
	d) Auto install and restart at a specific time			
	e) Auto install and restart without end-user control			
	f) Turn off automatic update by admin			
2	Configure Automatic Maintenance Wake Up			
3	Update Notification Level			
	a) Use default Windows update notifications			
	b) Turn off all, excluding restart warnings			
	c) Turn off all, including restart warnings			
4	Configure Fill Empty Content Urls			
	Configure Deferral Settings			
1	Configure Defers Feature Updates (0 - 365 Days)			

2	Pause Feature Updates (60 Days)			
3	Configure Deadline for Feature Updates			
4	Configure Defers Quality Updates			
5	Pause Quality Updates (35 Days)			
6	Configure Deadline for Quality Updates			
7	Configure Deadline for Grace Period			
8	Configure Deadline for No Auto Reboot			
9	Feature Update Uninstall Period			
	Configure Scheduling Settings			
1	Schedule Install Day			
2	Schedule Install Week			
3	Schedule Install Time			
	Configure Branching Settings			
1	Configure Update Branch			
	1. Semi-annual Channel (Targeted)			
	2. Windows Insider Build - Fast			
	3. Windows Insider Build - Slow			
	4. Release Windows Insider Build			
2	Manage Preview Builds			
	1. Disable Preview Builds			
	2. Disable Preview Builds once the next release is public			
	3. Enable Preview Builds			
3	Microsoft App Updates			
4	Configure WSUS Server URL instead of Microsoft Update			
5	Allow device to use Microsoft Update, Windows Server Update Services (WSUS), or Microsoft Store			
6	Allow Non Microsoft Signed Updates			
7	Alternate Intranet Server for Updates			
8	Exclude Drivers Update			
	Configure Administration & Network Settings			
1	Require Update Approval			
2	Disable UI/UX to Pause Windows Update			
3	Disable UI/UX to Scan Windows Update			
4	Allow Auto Update over Metered Network			
	Configure Scanning			
1	Detection Frequency			
2	Disable Dual Scan			
	Configure Restart & Notification			
1	Engaged Restart Deadline(Quality Updates)			
2	Engaged Restart Deadline(Feature Updates)			
3	Engaged Restart Snooze Schedule(Quality Updates)			
4	Engaged Restart Snooze Schedule(Feature Updates)			
5	Engaged Restart Transition Schedule(Quality Updates)			
6	Engaged Restart Transition Schedule(Feature Updates)			

7	Auto Restart Deadline Period(Quality Updates)			
8	Auto Restart Deadline Period(Feature Updates)			
9	Schedule Imminent Restart Warning			
10	Schedule Restart Warning			
11	Auto Restart Notification Schedule			
12	Auto Restart Required Notification Dismissal			
13	Disable Auto Restart Notification			
14	Set Cart Restart			
	Delivery Optimization			
	Configure Delivery Optimization via			
1	Windows CSP			
2	Agent Based			
	Configure Delivery Optimization to allow peer to peer delivery of updates			
1	Download Mode			
	1. Not Configured			
	2. HTTPS Only			
	3. LAN			
	4. Group			
	5. Internet			
	6. Simple			
	7. Bypass mode (Use BITS insted of Bypass mode)			
2	Restrict Peer Selection			
	1. Not Configured			
	2. Subnet Mask			
	3. Local Peer Discovery (DNS-SD)			
3	Group ID Source			
	1. Not Configured			
	2. Custom			
	3. AD Site			
	4. Authenticated domain SD			
	5. DHCP user option			
	6. DNS Suffix			
	7. AAD			
4	Configure Group ID			
	Configure Bandwidth Settings			
1	Bandwidth optimization type			
	1. Not configured			
	2. Absolute			
	3. Percetage			
	4. Percentage with Business Hours			
2	Maximum Background Download Bandwidth (in KB/s)			
3	Maximum Foreground Download Bandwidth (in KB/s)			
4	Maximum Background Download Bandwidth (percentage)			

5	Maximum Foreground Download Bandwidth (percentage)			
6	Configure Maximum Background Download Bandwidth			
	1. Business hours start			
	2. Business hours end			
	3. During business hours (in %) (0-100)			
	4. Outside business hours (in %) (0-100)			
7	Configure Maximum Foreground Download Bandwidth			
	1. Business hours start			
	2. Business hours end			
	3. During business hours (in %) (0-100)			
	4. Outside business hours (in %) (0-100)			
8	Delay Background Download from HTTP (in seconds)			
9	Delay Foreground Download from HTTP (in seconds)			
10	Monthly Upload Data Cap (GB)			
11	Minimum QoS for Background Downloads (in KB/s)			
	Configure Caching Settings			
1	Minimum RAM required for peer caching (in GB)			
2	Minimum disk size required for peer caching (in GB)			
3	Minimum content file size for peer caching (in MB)			
4	Minimum battery level required to upload (in %)			
5	Modify cache drive			
6	Maximum cache age (in seconds)			
7	Maximum cache size type			
	1. Not Configured			
	2. Absolute			
	3. Percentage			
8	Absolute maximum cache size (in GB)			
9	Maximum cache size (in %)			
10	VPN peer caching			
	1. Not Configured			
	2. Disabled			
	3. Enabled			
	Configure Local Server Setting			
1	Cache server host names			
2	Delay foreground download Cache Server fallback (in seconds)			
3	Delay background download Cache Server fallback (in seconds)			
	Configure Report Setting			
1	Collect Delivery Optimization Download and Upload statistics			
	Linux Desktop OS (Agent Based Protocol)			
	Configure the default global settings for Linux MDM agent to query and sync updates			
1	Configure Update Sync Interval			
2	Force Reboot Devices after Updates			
3	Auto Remove Packages			

4	Configure Update Schedule			
	1. Deploy Upon Approval			
	2. Deploy according to the following schedule			
	a) Update Time			
	b) Update Day			
	c) Update Week			
	Configure OS Update Policy			
1	Override Global OS Update Settings			
2	Enable OS Update and Patch Management			
3	OS Deferral Settings			
	Defer Updates			
1	Defer major software updates			
2	Defer minor software updates			
3	Defer non-os updates			
	Update Policy Settings			
1	Update Policy			
	a) Display in Dashboard & let IT Admins choose to publish the updates			
	b) Display in Dashboard & Queue in the Self-Service App			
2	Deferral Settings			
	1. Allow users to defer installation for number of times			
	2. Prompt users to install the updates every number of hours			
	Update Failure Handling			
1	Failure Handling			
	Mark as failed if the update is idle for number of hours			
	Retry failed updates for number of times			
	Continuously monitor and apply updates, security patches and policies to ensure endpoint compliance with regulatory or organizational security policies			
MDM Technical Specifications				
Sr No	**Mobile Device Management (MDM) for Laptops**	**Compliance (Yes/No)**	**Evidence**	**Remarks (If Any)**
Operating System Management Support				
1	Manage Windows Desktop OS			
2	Manage Linux OS			
3	BitLocker encryption on Windows OS			
MDM remote management software requirements:				
Architecture and General features				
1	The MDM remote management software should be completely web based(HTTPS console, web services/Rest API & Web sockets based communication, all using only one https port 443)			
2	The MDM Remote management software including the admin console should consist of central installation only and should not require any site level separate components to be installed.			

3	The MDM Remote management software should support granular, custom configurable admin user roles/profiles with the ability to map with AD.			
4	The MDM Device Agent should not open or make use of any local listening ports. All communication should be agent-initiated for security purposes.			
5	The scalability and sizing should be transparent using web servers and should work with any existing network load balancers, should not require any proprietary communicate gateways or middleware servers or proprietary components.			
6	Should have centralized dashboard depicting the hardware and software inventory, device status, health status, patch and vulnerability summary, alerts etc			
7	Should have dedicated views and modules for device management, asset management, software deployment including imaging, patch management, alert and incidents management, compliance management, preventive maintenance, mailer engine, advanced reporting.			
8	Should support all desired complex device configurations like multiple batteries monitoring, granular usb devices security policies, application whitelist and blacklist, power management, performance management, lockdown and hardening, service mode, shadowing, kiosk / restricted mode configuration etc			
9	Security Manager allows to set device lockdown and security setting like kiosk mode, USB Security Manager etc.			
10	Support for use of Enterprise CA signed certificate for SSL communication			
11	Ability to have multiple sessions using same admin username			
12	Should support location wise tracking of devices using GeoIP.			
13	The device remote control/shadowing should be web based using html5 viewer.			
14	Should provide audit reports specific for work from home or remote working scenarios			
15	In case of exit of an Employee (owing to retirement/death/any other reason) the MDM licenses, during the contract period, can be reallocated to other user.			
Installation & UI				
1	Solution should be capable to work On-Premises, on Cloud and Hybrid mode as well			
2	LAN, WAN & Internet scenarios to be supported			
3	Access anywhere "web based" login			
4	Active Directory Intergration			
5	API support			
Digital Workspace Support				
1	Bring your own device (BYOD)			
2	Corporate Owned fully supervised			
3	Corporate Owned and personally enabled			
4	Corporate owned single use dedicated mode			
Device Management features				

1	Full featured device information dashboard			
2	Device Discovery: Auto discovery of devices			
3	Device Inventory: List, Synchronization, Add, Edit & Delete			
4	Device details: Device dashboard, Current device configuration details, device hardware & software information			
5	Device control commands: Restart, Shutdown, Factory Reset, Inventory sync			
6	Device monitoring: On/off, Broker connection status			
Device baseline configuration/policies & Compliance tracking				
1	Support for both default & desired configurations, Device baseline configuration/policies creation, compliance tracking & monitoring, compliance report			
Management Software Features				
1	Multi level Group management support, Default Configurations for Group inheritance			
2	Task management, Template management, Task & Template Scheduling, Recurring tasks			
3	**Remote shadow and control devices:** Web based remote control , Prompt User for access control, Windows remote desktop sharing, Remote Shutdown, Sending Network Messages, Control a User Session, Service mode			
4	**Incident management including Device Monitoring & Preventive maintenance:** Monitoring Incidents Dashboard, Configure thresholds, System health, Trigger actions, Services, File system monitoring, Application & process monitoring, Registry key monitoring, Resource health monitoring, HDD health monitoring (SMART), Printer status, WMI events			
5	OTA upgrade patch management and device health monitoring			
6	**Asset Management:** Asset Dashboard; Data entry, importing asset lists (locations, user, dept.); Automatic Inventory updates of assets, Hardware Compliance, Detecting obsolete hardware (warranty/end of line), Achieving Software License Compliance, Software License Reports.			
Endpoint Controls				
1	Allow/Block taskbar			
2	Configure Users			
3	Configure File Manager Restrictions			
4	Allow/Block Apps			
5	Configure Startup App			
6	Configure Chrome Browser Settings			
7	Configure Edge Browser Settings			
8	Configure Kiosk App			
9	Configure Settings App - Show/Hide Selected Settings			
10	Enable/Disable Windows Accounts			
11	Enable/Disable App Manager			

12	Enable/Disable Cortana			
13	Enable/Disable Device Settings			
14	Enable/Disable Ease of Access			
15	Enable/Disable Extras			
16	Enable/Disable Gaming Settings			
17	Enable/Disable Network & Internet Settings			
18	Enable/Disable Personalization Settings			
19	Enable/Disable Privacy Settings			
20	Enable/Disable Surface Hub Settings			
21	Enable/Disable System Settings			
22	Configure System Settings			
23	Enable/Disable Time & Language Settings			
24	Enable/Disable Update & Security			
25	Enable/Disable User Account Settings			
26	Configure Bitlocker Encryption			
27	Configure Windows Hello			
28	Configure Windows Defender			
29	Configure Windows OS Updates			
30	Configure Patch Management			
31	Configure Custom Payload			
32	Configure Start Layout Settings			
33	Configure Display Settings			
34	Configure Application Settings			
35	Allow/Restrict Camera			
36	Allow/Restrict Microsoft Account Connection			
37	Allow/Restrict Adding of Non Microsoft Accounts			
38	Allow/Restrict Sync Settings across Devices			
39	Allow/Restrict Reset Devices			
40	Allow/Restrict Developer Unlock			
41	Allow/Restrict Location Services			
42	Windows OS & Driver Updates			
43	Windows OS & Driver Updates			
44	Configure Peripheral Settings			
45	Configure Local Admin Privileges			
46	Remote App Installation via Micrsoft Store			
47	Remote UWP App Installtion			
48	Remote MSI App Installtion			
49	Remote EXE App Installtion			
50	Remote Powershell Script Execution			
Audit & Reporting				
1	Audit Logs			
2	Data Usage Report			
3	Device Inventory Report			
4	Device Vitals Report			

5	Location History Report			
6	App Version Reports			
7	Remote Sessions Report			
10	Unlock Attempts Report			
11	FileDock Analytics			
12	Enterprise Store Report			
13	Device Availability Report			
14	Screen Time Report			
15	GeoFence Logs			
16	Battery History Report			
17	WorkFlow Report			
18	Connectivity History			
Support				
1	Live Chat Support			
2	Email Support			
3	Dedicated Account Manager			
4	Technical Support			
Content Management				
1	Define Paths for Content Sharing			
2	Remotely push files and folders			
3	Digital signage kiosk (Presentation Mode)			
4	Push content as screensaver			
5	Configure Screensaver Settings			
6	Set Interval Time for changing content			
7	Configure Device Orientation			
8	Configure Play On-Demand Shortcut			
9	Google Drive Integration for Content Sharing			
10	Content Management Storage			
Remote Access				
9	Scripts - Win			
10	Remote Cast - Win			
11	Remote Control - Win			
Workflows				
1	Schedule Switch Profile			
2	GeoFence based Switch Profile			
3	Schedule Lock/Unlock			
4	Schedule Reboot			
5	Schedule Clear App Data			
6	Schedule Clear Browser Cache			
7	Schedule ProSurf Clear Cache in iOS			
8	Schedule Switch Presentation			
9	Schedule Application Publish			
10	Set Battery Compliance			
11	Set Geo-Fence Compliance			

12	Set Data Usage Compliance			
13	Set Security Incidents Compliance			
14	Set Inactivity Compliance			
15	Storage Compliance			
16	Schedule Device Reports			
17	Schedule Broadcast Messages			
18	Schedule Clear Files & Broadcast Messages			
19	Schedule Single App Mode Profile			
Administrators & Roles				
1	Technicians/Administrators			
2	Pre-Defined Role Based Access Controls			
3	Custom Role Based Access Controls			
4	Assign Admins to Specific Device Groups			
5	Multi Factor Authentication			
6	Configure Passcode Policy for Dashboard Access			
7	Configure Session Time out for Dashbaord Access			
8	Configure SAML			
Integrations				
1	ITSM Integration			
2	Developer API			
3	Active Directory			
4	Office 365			
5	JIRA			
6	SIEM Integration			
7	Other Security Solutions as applicable			
KMS Technical Specifications				
#	**BitLocker Key Management Solution (KMS)**	**Compliance (Yes/No)**	**Evidence**	**Remarks (If Any)**
1	The proposed solution must provide centralized management of BitLocker encryption across all Windows endpoints in the enterprise environment.			
2	It should support policy enforcement, key escrow, compliance reporting, and secure recovery of BitLocker keys.			
3	Must support centralized configuration and enforcement of BitLocker policies including encryption method, algorithm (AES 128/256 XTS), TPM enforcement, startup authentication (TPM only, TPM + PIN, TPM + USB), and silent encryption deployment without user intervention			
4	The solution should enforce full-disk encryption policies remotely and provide real-time status monitoring of BitLocker deployment and encryption progress on all endpoints.			
5	Must securely store BitLocker recovery keys in a centralized repository. Admins should be able to search and retrieve keys via a secure web-based console, with role-based access controls (RBAC) and audit logging of key access.			

6	Should support automatic rotation of recovery keys after use, device transfer, or policy violation, and offer secure offline export options for long-term archival.			
7	Must provide detailed reports on encryption compliance, non-compliant devices, and recovery key escrow status. Reports should be exportable (PDF/Excel/CSV) and support automated scheduling.			
8	The solution should offer configurable alerts for devices not encrypted, policy violations, or failed encryption attempts, with notifications via email or admin dashboard.			
9	Full audit trail of administrative activities, especially key retrieval events, with searchable history and export capabilities for audit compliance.			
10	Should integrate with Microsoft AD and/or Azure AD for identity and policy binding. Also must support event and log export to SIEM platforms			
11	Recovery keys must be stored in encrypted form (AES-256 or higher). Admin access to the management console must support multi-factor authentication (MFA) and session timeout enforcement.			
12	A self-service portal for end-users to securely retrieve their own recovery key, protected by MFA, is desirable but not mandatory.			
13	Support the creation of multiple encryption and key management profiles based on department, user role, or location.			

ANNEXURE 11 – DELIVERY LOCATIONS

(To be submitted in the Bidder's letter head)

[TO BE INCLUDED IN 'COVER – A' ELIGIBILITY CUM TECHNICAL BID ENVELOPE]

Below are the delivery locations:

DC LOCATION:

UNITED INDIA INSURANCE COMPANY LIMITED

M/s. Sify Technologies Ltd

Airoli DC, Reliable Plaza, Plat No-K10, Kalwa Block, TTL Industrial Area, Thane,

Mumbai-400 708

DR LOCATION:

UNITED INDIA INSURANCE COMPANY LIMITED

Ctrls Datacenters Ltd.,

16, Software Units Layout, Madhapur (Hitech City), Hyderabad, Telangana – 500 081.

Authorized Signatory Name Designation Office Seal Place:

Date:

ANNEXURE 12 - PRE INTEGRITY PACT (FORMAT)

(Bidders to submit 2 (two) copies of integrity pact in ₹ 100 stamp paper)

[TO BE INCLUDED IN 'COVER – A' ELIGIBILITY CUM TECHNICAL BID ENVELOPE]

Ref. <>

Date:

1 General

This pre-bid-pre-contract Agreement (hereinafter called the Integrity Pact) is made at

_____place _____on _____ day of the month of _____, 2025 between United India Insurance Company Limited, having its Head Office at 24, Whites Road, Chennai – 600 014 (hereinafter called the "BUYER/UIIC", which expression shall mean and include, unless the context otherwise requires, its successors and assigns) of the First Part and M/s._____ represented by Shri./Smt._____, Chief Executive Officer (hereinafter called the "BIDDER/SELLER" which expression shall mean and include, unless the context otherwise requires, his successors and permitted assigns) of the Second Part.

WHEREAS the BUYER proposes to issue RFP for supply, installation and maintenance of firewall and the BIDDER/SELLER is willing to offer/has offered the services and WHEREAS the BIDDER is a private company/Public company/Government undertaking/partnership/registered export agency, constituted in accordance with the relevant law in the matter and the BUYER is a corporation set up under an Act of Parliament.

NOW, THEREFORE,

To avoid all forms of corruption by following a system that is fair, transparent and free from any influence /prejudiced dealing prior to, during and subsequent to the currency of the contract to be entered into with a view to:

- Enabling the BUYER to obtain the desired said stores/equipment/services at a competitive price in conformity with the defined specifications by avoiding the high cost and the distortionary impact of corruption on Public procurement and
- Enabling BIDDERs to abstain from bribing or indulging in any corrupt practice in order to secure the contract by providing assurance to them that their competitors will also abstain from bribing and other corrupt practices and the BUYER will commit to prevent corruption in any form by its officials by following transparent procedures.

The parties hereto hereby agree to enter into this integrity Pact and agree as follows:

2 Commitments of the BUYER

2.1 The BUYER undertakes that no official of the BUYER, connected directly or indirectly with the contract, will demand, take a promise for or accept, directly or through intermediaries, any bribe, consideration, gift, reward, favour or any material or immaterial benefit or any other advantage from the BIDDER, either for themselves or for any person, organization or third party related to the contract in exchange for an advantage in the bidding process, bid evaluation, contracting or implementation process related to the contract.

2.2 The BUYER will during the pre-contract stage, treat all BIDDERs alike, and will provide to all BIDDERs the same information and will not provide any such information to any particular BIDDER which could afford an advantage to that particular BIDDER in comparison to other BIDDERs.

2.3 All the officials of the BUYER will report to the appropriate Government office any attempted or completed breaches of the above commitments as well as any substantial suspicion of such a breach.

2.4 In case any such preceding misconduct on the part of such official(s) is reported by the BIDDER to the BUYER with full and verifiable facts and the same is prima facia found to be correct by the BUYER, necessary disciplinary proceedings, or any other action as deemed fit, including criminal proceedings may be initiated by the BUYER and during such a period shall be debarred from further dealings related to the contract process. In such a case while an enquiry is being conducted by the BUYER the proceedings under the contract would not be stalled.

3 Commitments of BIDDERs

The BIDDER commits itself to take all measures necessary to prevent corrupt practices, unfair means and illegal activities during any stage of its bid or during any pre-contract or post-contact stage in order to secure the contract or in furtherance to secure it and in particular commit itself to the following:

3.1 The BIDDER will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any officials of the BUYER, connected directly or indirectly with bidding process, or to any person, organization or third party related to the contract in exchange for any advantage in the bidding, evaluation, contracting and implementation of the contract.

3.2 The BIDDER further undertakes that it has not given, offered or promised to give, directly or indirectly any bribe , gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the BUYER or otherwise in procuring the Contract or forbearing to do or having done any act in relation to the obtaining or execution of the contract or any other contract with the Government for showing or forbearing to show favour or disfavour to any person in relation to the contract or any other contract with the Government.

3.3 BIDDERs shall disclose the name and address of agents and representatives and Indian BIDDERs shall disclose their foreign principals or associates.

3.4 BIDDERs shall disclose the payments to be made by them to agents/brokers or any other intermediary, in connection with this bid/contract.

3.5 The BIDDER further confirms and declares to the BUYER that the BIDDER is the original manufacture/integrator/authorized government sponsored export entity of the defence stores and has not engaged any individual or firm or company whether Indian or foreign to intercede, facilitate or any way to recommend to the BUYER or any of its functionaries, whether officially or unofficially to the award of the contract to the BIDDER, or has any amount been paid, promised or intended to be paid to any such individual, firm or company in respect of any such intercession, facilitation or recommendation.

3.6 The BIDDER, either while presenting the bid or during pre-contract negotiations or before signing the contract, shall disclose any payments he has made, is committed to or intends to make to

Officials of the BUYER or their family members, agents, brokers or any other intermediaries in connection with contract and the details of services agree upon for such payments.

3.7 The BIDDER will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, bid evaluation, contracting and implementation of the contract.

3.8 The BIDDER will not accept any advantage in exchange for any corrupt practice, unfair means and illegal activities.

3.9 The BIDDER shall not use improperly, for purposes of competition or personal gain or pass on the others, any information provided by the BUYER as part of the business relationship, regarding plans, technical proposals and business details, including information contained in any electronic data carrier. The BIDDER also undertakes to exercise due and adequate care lest any such information is divulged.

3.10 BIDDER commits to refrain from giving any complaint directly or through any other manner without supporting it with full and verifiable facts.

3.11 The BIDDER shall not instigate or cause to instigate any third person to commit any of the actions mentioned above.

3.12 if the BIDDER or any employee of the BIDDER or any person acting on behalf of the BIDDER, either directly or indirectly, is a relative to any of the officers of the BUYER or alternatively, if any relative of the officer of the BUYER has financial interest/stake in the BIDDER's firm, the same shall be disclosed by the BIDDER at the time of filling of tender. The term 'relative' for this purpose would be as defined in Section 2 (77) of the Companies Act, 2013.

3.13 The BIDDER shall not lend to or borrow any money from or enter into any monetary dealings or transactions, directly or indirectly, with any employee of the BUYER.

4 Previous Transgression

4.1 The BIDDER declares that no previous transgression occurred in the last three years immediately before signing of this integrity Pact, with any other company in any country in respect of any corrupt practices envisaged hereunder or with any Public Sector Enterprise in India or any Government Department in India that could justify BIDDER's exclusion from the tender process.

4.2 The BIDDER agrees that if it makes incorrect statement on this subject, BIDDER can be disqualified

from the tender process or the contract, if already awarded, can be terminated for such reason.

5 Earnest Money (Security Deposit)

5.1 While submitting commercial bid, the BIDDER shall deposit an amount of ₹ 30,00, 000/- (Rupees Thirty Lakh only) as Earnest Money/Security Deposit, with the BUYER through any of the following instrument.

(i) in the form of electronic credit only to UIIC Bank Account.

(ii) A confirmed guarantee by an Indian Nationalised Bank, promising payment of the guaranteed sum to the BUYER immediately on demand without any demur Whatsoever and without seeking any reasons whatsoever. The demand for payment by the BUYER shall be treated as conclusive proof of payment.

(iii) The Earnest Money/Security Deposit shall be valid for a period of 3 months OR the complete conclusion of the contractual obligation to the complete satisfaction of both the buyer and bidder, including the warranty period, whichever is later.

(iv) In case of the successful BIDDER a clause would also be incorporated in the Article pertaining to Performance Bond in the Purchase Contract that the provision of Sanctions for Violation shall be applicable for forfeiture of Performance Bond in case of a decision by the BUYER to forfeit the same without assigning any reason for imposing sanction for violation of this Pact.

(v) No interest shall be payable by the BUYER to the BIDDER on Earnest Money/Security Deposit for the period of its currency.

(vi) A confirmed guarantee by an Indian Nationalised Bank, promising payment of the guaranteed sum to the BUYER immediately on demand without any demur whatsoever and without seeking any reasons whatsoever. The demand for payment by the BUYER shall be treated as conclusive proof of payment.

6 Sanctions for Violations

6.1 Any breach of the aforesaid provision by the BIDDER or any one employed by it or acting on its behalf (whether with or without the knowledge of the BIDDER) shall entitle the BUYER to take all or any one of the following actions, wherever required:

i. To immediately call off the pre contract negations without assigning any reason or giving any compensation to the BIDDER. However, the proceedings with other BIDDER(s) would continue

ii. The Earnest Money Deposit (in pre-contract stage) and /or Security Deposit/Performance Bond) (after the contract is signed) shall stand forfeited either fully or partially, as decided by the BUYER and the BUYER shall not be required to assign any reason therefore.

iii. To immediately cancel the contract, if already signed, without giving any compensation to the BIDDER

iv. To recover all sums already paid by the BUYER, and in case of Indian BIDDER with interest thereon at 2% higher than the prevailing Prime Lending Rate of State Bank of India, while

in case of a bidder from a country other than India with interest thereon at 2% higher than LIBOR. If any outstanding payment is due to the bidder from the buyer in connection with any other contract for any other stores, such outstanding payment could also be utilized to recover the aforesaid sum and interest.

v. To encash the advance bank guarantee and performance bond/warranty bond, if furnished by the BIDDER, in order to recover the payments, already made by the BUYER along with interest.

vi. To cancel all or any other Contracts with the BIDDER, the BIDDER shall be liable to pay compensation for any loss or damage to the BUYER resulting from such cancellation/rescission and the BUYER shall be entitled to deduct the amount so payable from the money(s) due to the BIDDER

vii. To debar the BIDDER from participating in future bidding processes of the buyer or its associates or subsidiaries for minimum period of five years, which may be further extended at the discretion of the BUYER.

viii. To recover all sums paid in violation of this Pact by BIDDER(s) to any middleman or agent or broker with a view to securing the contract.

ix. In cases where irrevocable Letters of Credit have been received in respect of any contract signed by the BUYER with BIDER, the same shall not be opened.

x. Forfeiture of Performance Bond in case of decision by the BUYER to forfeit the same without assigning any reason for imposing sanction for violation of this Pact.

6.2 The BUYER will be entitled to take all or any of the actions mentioned at para 6.1(i) to (x) of this Pact also on the commission by the BIDDER or any one employed by it or acting on its behalf (whether with or without the knowledge of the BIDDER), of an offence as defied in Chapter IX of the Indian Penal code, 1860 or Prevention of Corruption Act, 1988 or any other statute enacted for prevention of corruption.

7 The decision of the BUYER to the effect that a breach of the provision of this Pact has been committed by the BIDDER shall be final and conclusive on the BIDDER. However, the BIDDER can approach the independent Monitor(s) appointed for the purposes of this Pact.

8 Fall Clause

8.1 The BIDDER undertakes that it has not supplied/is not supplying similar products /systems or subsystems at a price lower than that offered in the present bid in respect of any other Ministry/Department of the Government of India or PSU and if it is found at any stage that similar product/systems or sub systems was supplied by the BIDDER to any other Ministry/Department of the Government of India or a PSU at a lower price, then that very price, with due allowance for elapsed time, will be applicable to the present case and the difference in the cost would be refunded by the BIDDER to the BUYER, if the contract has already been concluded.

9 Independent Monitors

9.1 The BUYER is in the process of appointing Independent Monitors (hereinafter referred to as

Monitors) for this Pact in consultation with the Central Vigilance Commission.

9.2 The task of the Monitors shall be to review independently and objectively, whether and to what extent the parties comply with the obligations under this Pact.

9.3 The Monitors shall not be subject to instruction by the representatives of the parties and perform their functions neutrally and independently.

9.4 Both the parties accept that the Monitors have the right to access all the documents relating to the project/procurement, including minutes of meetings.

9.5 As soon as the Monitor notices or has reason to believe, a violation of the Pact, he will so inform the Authority designated by the BUYER

9.6 The BIDDER(s) accepts that the Monitor has the right to access without restriction to all Project documentation of the BUYER including that provided by the BIDDER. The BIDDER will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documents. The same is applicable to Subcontractors. The Monitor shall be under contractual obligation to treat the information and documents of the BIDDER/Subcontractor(s) with confidentiality

9.7 The BUYER will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the parties. The parties will offer to the Monitor the option to participate in such meetings

9.8 The Monitor will submit a written report to the designed Authority of the BUYER within 8 to 10 weeks from the date of reference or intimation to him by the BUYER/BIDDER and should the occasion arise, submit proposals for correcting problematic situations.

10 Facilitation of Investigation

In case of any allegation of violation of any provision of this Pact or payment of commission, the BUYER or its agencies shall be entitled to examine all the documents including the Books of Accounts of the BIDDER and the BIDDER shall provide necessary information and documents in English and shall extend all possible help for the purpose of such examination.

11 Law and Place of Jurisdiction

12 This Pact is subject to Indian Law. The place of performance and jurisdiction is the seat of the BUYER.

13 Other Legal Actions

The action stipulated in this integrity Pact are without prejudice to any other legal action that may follow in accordance with the provisions of the extant law in force relating to any civil or criminal proceedings.

14 Validity

14.1 The validity of this Integrity Pact shall be from date of its signing and extend upto 3 years or the

complete execution of the contract to the satisfaction of both the BUYER and the BIDDER/Seller, including warranty period, whichever is later in case BIDDER is unsuccessful, this integrity Pact shall expire after six months from the date of the signing of the contract.

14.2 Should one or several provisions of the Pact turn out to be invalid, the remainder of this Pact shall remain valid. In this case, the parties will strive to come to an agreement to their original intentions.

15 The parties hereby sign this integrity Pact, at _____on _____

(a) for & on behalf of United India Insurance Co. Ltd

(a) for & on behalf of (BIDDER'S NAME)

DEPUTY GENERAL MANAGER

- - _____ - - _____

In the presence of: Witnesses - 1:

Witnesses - 2:

In the presence of:

Witnesses - 1:

Witnesses - 2:

ANNEXURE 13 – LAND BORDER WITH INDIA

(To be submitted in the Bidder's/OEM'S letterhead)

[TO BE INCLUDED IN 'COVER – A' ELIGIBILITY CUM TECHNICAL BID ENVELOPE]

Ref. No: <>

To

The Deputy General Manager
Information Technology Department
United India Insurance Co. Ltd.
Head Office, 24, Whites Road,
Chennai – 600014.

Subject: Offer for RFP Ref. No. 0<>

Dear Sir/Madam,

I have read Office Memorandum F.No.6/18/2019-PPD dated <> issued by the Ministry of Finance, Department of Expenditure, Public Procurement Division inserting Rule 144 (xi) in GFRs 2017 which defines clauses regarding restrictions or procurement from a bidder of a country which shares a land border with India. I certify that _____(Bidder / OEM Name) is not from such a country or, if from such a country, has been registered with the competent authority, I certify that this bidder / OEM fulfils all requirements in this regard and is eligible to be considered. [Where applicable, evidence of valid registration by the competent authority shall be attached.]"

Authorized Signatory Name Designation Office

Seal Place:

Date:

ANNEXURE 14 – PREBID QUERY FORMAT

Date:

To

The Deputy General Manager
Information Technology Department
United India Insurance Co. Ltd.
Head Office, 24, Whites Road,
Chennai – 600014.

Subject: Queries w.r.t. <>

Note: The queries may be communicated only through e-mail to email id **rfp.infra@uiic.co.in**. Responses of queries will be uploaded in UIIC website or emailed to concerned bidder. No queries will be accepted on telephone or through any means other than e-mail. **The queries shall be sent in .xls/.xlsx format with below fields only.**

S.No	Bidder Name	Page No (Tender Ref)#	Point / Section	Existing Clause	Query	Contact Details
1.						
2.						
3.						
4.						

Authorized Signatory Name Designation Office

Seal Place:

Date:

ANNEXURE 15 - BID SUBMISSION CHECK LIST – FOR BIDDERS

S#	Document	Attached (Yes/No)	Page#
COVER A			
1	Tender Fee remittance details		
2	Letter of Authorization as per Annexure 1		
3	No Blacklisting Declaration as per Annexure 2		
4	Manufacturers Authorization Format - ANNEXURE 3A (or) Undertaking for being the OEM of the offered solution as per ANNEXURE 3B		
5	Statement of Nil deviation as per Annexure 4		
6	Proof of Earnest Money Deposit (EMD) amount deposited in UIIC Account / Bank Guarantee for EMD as per Annexure 5		
7	Eligibility Criteria Declaration Form as per Annexure 6 and Supporting documents as detailed in Annexure 6.		
8	Non-Disclosure Agreement as per Annexure 8		
9	Compliance Statement for the Minimum Functional & Technical Specifications as detailed in Annexure 9.		
10	Delivery Locations as per ANNEXURE 10		
11	Pre-Contract Integrity Pact as per Annexure 11 in stamp paper (2 copies)		
12	Land Border with India as per Annexure 12 from OEM / Bidder		
13	Hardware End of Life and Support as per Annexure 15		
14	Project Team Profile (Individual) Detailed as per Annexure 16		
15	Performance certificate as per Annexure 18		
16	Proposed Solution With Architecture as per ANNEXURE 18		

17	Certificate For Local Content as per ANNEXURE 19		
18	Unpriced BOM as per Annexure 20.		
19	IT & IS GUIDELINESS as per Annexure 21		
20	Authorized signatory of the Bidder signing the Bid Documents should be empowered to do so. Proof in the form of letter signed by a Director or Company Secretary to be attached.		
21	Proof of Power of Attorney of OEM		
22	Supporting Technical documents, brochures, data sheet etc.,		
COVER B			
1	Commercial Bid as per Annexure 7, should include the sum total of all the line items mentioned in Annexure 20 as per the respective the subject line		

Authorized Signatory Name Designation Office

Seal Place:

Date:

ANNEXURE 16 – HARDWARE END OF LIFE AND SUPPORT DECLARATION

< To be submitted in the OEM's letter head and should be signed by Authorized Signatory of the OEM >

[TO BE INCLUDED IN 'COVER – A' ELIGIBILITY CUM TECHNICAL BID ENVELOPE]

Ref. No: <>

To

The Deputy General Manager
Information Technology Department
United India Insurance Co. Ltd.
Head Office, 24, Whites Road,
Chennai – 600014.

Subject: Offer for RFP Ref. No. <>

Dear Sir/Madam,

We _____(OEM & address) have supplied _____(Hardware Make / model and quantity). We confirm that the Supplied hardware will not be end-of-life / End-of-sale during contract period and will be under support from the date of PO to next 7 years. The bug/Patches and release will be available to UIIC for above mentioned 7 years duration.

Authorized Signatory Name Designation Office

Seal Place:

Date:

ANNEXURE 17 – PROJECT TEAM PROFILE (INDIVIDUAL) DETAILED

(To be submitted in the Bidder's letter head)

[TO BE INCLUDED IN 'COVER – A' ELIGIBILITY CUM TECHNICAL BID ENVELOPE]

1	**Name**			
a	Brief Introduction (in bullets)			
2	Date of Birth			
3	Phone Number			
4	Position in the firm			
5	Total years of post-qualification work experience			
6	**Employment Record**			
	Company Name	Positions Held	Duration	**Clients Worked**
6.1				
6.2				
6.3				
6.4				
6.5				
7	Number of years the firm with			
8	**Details of relevant assignments undertaken (include both past and current employment projects and highlight BFSI experience, if any)**			
	(Provide scope, duration, client name and us of assignment) stat			
a	Year			
	Location			
	Client Name			
	Main project title and features			
	Position held			
	Activities performed			
b	Year			
	Location			
	Client Name			
	Main project title and features			
	Position held			
	Activities performed			
9	Education			
	Degree		**Institution**	

	Obtained	**Year of**			
9.1		**Degree obtained**			
9.2					
9.3					
9.4					
9.5					
10	Certification				
	Degree Obtained	**Year of Degree obtained**	**Institution**		
10.1					
10.2					
10.3					
10.4					
10.5					

Authorized Signatory Name Designation Office

Seal Place:

Date:

ANNEXURE 18 – PERFORMANCE CERTIFICATE

(To be submitted on letter head of the issuing company)

[TO BE INCLUDED IN 'COVER – A' ELIGIBILITY CUM TECHNICAL BID ENVELOPE]

Ref. No: <>

To
The Deputy General Manager
Information Technology Department
United India Insurance Co. Ltd.
Head Office, 24, Whites Road,
Chennai – 600014.

Subject: Offer for RFP Ref. No. <>

This is to certify that M/s _____ has supplied, installed and successfully Maintained/maintaining _____ (Name of the Solution) originally developed by _____ (OEM name) to our organization since_____ for _____ (brief Purpose/Objective of the Solution).

The solution has been implemented for _____no. of users.

The services provided by the M/s _____ are satisfactory.

The certificate has been issued on the specific request of the company.

Authorized Signatory Name Designation Office

Seal

Place:

Date:

ANNEXURE 19 –CERTIFICATE FOR LOCAL CONTENT

[TO BE INCLUDED IN 'COVER – A' ELIGIBILITY CUM TECHNICAL BID ENVELOPE]

<Certificate from the statutory auditor or cost auditor of the company (in case of companies) or from a practicing cost accountant or practicing chartered accountant (in respect of suppliers other than companies) giving the percentage of local content, on their letter head with Registration Number with seal.>

Ref. No:

To
The Deputy General Manager
Information Technology Department
United India Insurance Co. Ltd.
Head Office, 24, Whites Road,
Chennai – 600014.

Subject: Offer for RFP Ref. No."<>" This is to certify that proposed ___<product details> is having the local content of _____% as defined in the above-mentioned RFP. The details of location(s) at which the local value addition is made are as under

Product Details		**Classification (Class-I local supplier / Class-II Local Supplier)**	**Name of Place where local value addition is made**
Make	**Model No.**		

I/We further certify that, in case we are awarded an order against this tender, the supplies against such order will comply with above indicated Minimum Local Content.

Signature of Statutory Auditor/Cost Auditor/
Name/Company:
Registration Number:
Seal COUNTER-SIGNED:

BIDDER **OEM**

Name & Signature of authorized signatory (In the capacity of) Duly authorized to sign bid for and on behalf of Bidder.	**Name & Signature of authorized signatory** (In the capacity of) Duly authorized to sign for and on behalf of OEM

ANNEXURE 20 –BILL OF MATERIALS

[TO BE INCLUDED IN 'COVER – A' ELIGIBILITY CUM TECHNICAL BID ENVELOPE]

Important Instructions: All Bidders have to compulsorily adhere to the following:

I	**Overall**
1	The bidder is expected to quote the costs for all items required for fully complying with the requirements of the RFP and the addenda in the respective sections of the price bid. The prices for the respective sections would be deemed to include all components required to successfully implement and maintain the solution for the contract period.
2	UIIC is not responsible for any arithmetic errors in the commercial bid details sheet committed by the shortlisted bidders, however, if there are any computational errors UIIC will evaluate the Bid as per provisions contained under RFP document.
3	The bidder is expected to specify the type of licenses along with the details with respect to quantity/rate/etc., wherever applicable
4	In case the bidder includes/combines any line item as part of any other line item in the commercial bid, then this has to be clearly mentioned in the description indicating the line item which contains the combination
5	The bidder has to quote for each line item. If any line item is part of the solution proposed in the RFP response, it has to be referenced. If it is not applicable, then the Bidder has to mention Not Applicable (NA).
6	Tax (GST) information is to be mentioned separately in this Bill of Material. The TAX TYPE (GST) and PERCENTAGE should be clearly mentioned in the masked and the unmasked versions of the Bill of Materials.
7	The Bidder may insert additional line items as applicable based on the solution offered in the respective tabs
8	The masked Bill of Materials which would be submitted as part of the Eligible cum Technical criteria, should contain **"XX"** for ALL the corresponding to the values that will be present in the unmasked Bill of Material that will be part of the Commercial submission.
8	The Bidders should quote as per the format of Bill of Materials **ONLY** and a masked replica of the Bill of Materials should be enclosed in the technical bid.
9	Bidder is required to cover component by component licensing details for each of the hardware and software components proposed to UIIC.
11	Quantities mentioned in Year 2 should be incremental over Year 1, Year 3 should be incremental over Year 2 and so on.
12	All amounts in the Bill of Material should be in INR
II	**Software**
1	The bidder has to quote for each line item. If any line item is part of the solution proposed in the RFP response, it has to be referenced. If it is not applicable, then the Bidder has to mention Not Applicable (NA).
2	The Bidder can insert additional line items as applicable based on the solution offered in the various tabs
3	The license type has to be clearly described in the description column
4	All installation charges for application, database and OS have to be quoted separately, as applicable.
III	**Hardware DC - DR**
1	The description for all **hardware** should strictly contain the following items in the same order:
	a. Make / Model of the Hardware
	b. Processor quantity, frequency, Cache memory,
	c. Maximum memory capacity, quoted memory
	d. Operating system
	e. NIC quantity, make

	f. Storage capacity
	g. Other critical components
2	The bidder has to quote for each line item. If any line item is part of the solution proposed in the RFP response, it has to be referenced. If it is not applicable, then the Bidder has to mention NA.
3	Any installation & commissioning charges for hardware have to be quoted separately
IV	**Waranty and AMC**
1	All the hardware proposed should by covered under warranty for a minimum period of 3 years; Post this the bidder should quote AMC for the remaining period of the contract
2	All the software proposed should be covered under warranty for a minimum period of 3 year; Post this the bidder should quote ATS for the remaining period of the contract
3	The AMC and ATS cost for individual hardware/applications/database/OS has to be quoted in separate line items in this section. The Bidder has to create additional line items in this section if required
4	The Tax details are to be mentioned separately as per the RFP guidelines.

The Bidder is expected to quote the costs for all items required for fully complying with the requirements of the RFP in the respective sections of the price bid. The prices for the respective sections would be deemed to include all components required to successfully implement and maintain the solution for the period of the contract

DC-DR SOLUTION COST

#	Component	Solution OEM	Quantity	Year 1		Year 2		Year 3		Year 4		Year 5		Total 5 Year Cost (INR)	Taxes As applicable (INR)	Grand Total (INR)
				Unit Price (INR)	Total Price (INR)	Unit Price (INR)	Total Price (INR)	Unit Price (INR)	Total Price (INR)	Unit Price (INR)	Total Price (INR)	Unit Price (INR)	Total Price (INR)			
1	Hardware		As per scope	x	x	x	x	x	x	x	x	x	x			
2	DLP Software Licenses		As per scope													
3	EDR Software Licenses		As per scope													
4	Data Discovery & Classification Software Licenses		As per scope													
5	MDM For Laptops Software Licenses		As per scope													
6	Patch Management Software Licenses		As per scope													
7	KMS Software Licenses		As per scope													

#	Component	Solution OEM	Quantity	Year 1		Year 2		Year 3		Year 4		Year 5		Total 5 Year Cost (INR)	Taxes As applicable (INR)	Grand Total (INR)
				Unit Price (INR)	Total Price (INR)	Unit Price (INR)	Total Price (INR)	Unit Price (INR)	Total Price (INR)	Unit Price (INR)	Total Price (INR)	Unit Price (INR)	Total Price (INR)			
8	One Time Implementation Cost		One Time	x	x	x	x	x	x	x	x	x	x			
9	Facility Management Services (FMS) - L1 Resource		As per scope													
10	Facility Management Services (FMS) - L2 Resource		As per scope													
11	Facility Management Services (FMS) - Project Coordinator		As per scope													
12	Annual Maintenance Contract (AMC)		As per scope	x	x	x	x	x	x	x		x				
13	Any Other, (Please specify)															
Grand Total (INR, incl. all components)																

PRICE DISCOVERY FOR ADDITIONAL LICENSES

#	Component	Solution OEM	Quantity	Year 1		Year 2		Year 3		Year 4		Year 5		Total 5 Year Cost (INR)	Taxes As applicable (INR)	Grand Total (INR)
				Unit Price (INR)	Total Price (INR)	Unit Price (INR)	Total Price (INR)	Unit Price (INR)	Total Price (INR)	Unit Price (INR)	Total Price (INR)	Unit Price (INR)	Total Price (INR)			
1	DLP Software Licenses		100													
2	EDR Software Licenses		100													
3	Data Discovery & Classification Software Licenses		100													
4	MDM For Laptops Software Licenses		100													
5	Patch Management Software Licenses		100													
6	Any Other, (Please specify)															
Grand Total (INR, incl. all components)																

NOTE:

- The Total Cost of Ownership (TCO) shall be total of the "DC-DR SOLUTION COST" and the cost of "PRICE DISCOVERY FOR ADDITIONAL LICENSES"
- Bidder must propose the additional license cost for the 5 years of contract period in the above format (In case of future requirement)

- The Bidder is expected to provide a detailed break up of all products and services that are under the scope of facilities management as part of the technical bid, in the technical bill of materials i.e. the above format is expected to be replicated for each item to be covered under the scope of facilities management
- The quantity mentioned above is for price identification purpose only and additional licenses will be procured on actual requirement basis.

ANNEXURE 21 – IT & IS GUIDELINESS

[TO BE INCLUDED IN 'COVER – A' ELIGIBILITY CUM TECHNICAL BID ENVELOPE]

Ratings	Classification	Description
M	Mandatory	This requirement is compulsory and must be satisfied in its entirety
E	Essential	This requirement is a necessary feature and carries high weightage
O	Optional	Optional requirement and carries low weightage

*Remarks to be furnished in case the bidder response is "No (N)", all responses may be reviewed as and when necessary

Security Access Control:

SNO	Requirement Description	Requirement Classification (M/E/O)	Bidder Response (Y/N)	Remarks
1	Two-factor authentication: Implement a strong authentication mechanism to verify the identity of proposed solution accessing system	M		
2	Role-based access controls: Define access privileges based on job roles to limit access to sensitive data only to authorized personnel	M		
3	Password policies: Enforce strong password policies to ensure secure access to systems	M		

Data Security:

SNO	Requirement Description	Requirement Classification (M/E/O)	Bidder Response (Y/N)	Remarks
1	Encryption in transit: Require the use of secure protocols (such as TLS) to protect data transmitted between systems and endpoints	M		
2	Encryption at rest: Encrypt sensitive data stored within databases, file systems, or any other storage systems to protect against unauthorized access in case of a data breach	M		
3	Data retention and disposal: Establish policies and procedures for retaining and disposing	M		
4	Platform to ensure Sensitive information like AADHAAR number and other PII information to be masked or encrypted in the database	M		
5	Audit and Compliance Management: Platform to enable suitable information security / cyber security and secure configuration in respect of the components, and utilities in the system, as per requirement of UIIC from time to time Continuous risk assessment and control process to be conducted and probability of each risk along with impact to be evaluated and to be provided proactively periodically to UIIC	M		
6	Bidder should comply with all the guidelines issued by IRDAI/DFS/DoT/TRAI/Govt of India, IT ACT,	M		

	Statutory requirements and any other regulatory authority from time to time at no additional cost to UIIC and should adhere to the security policies set up by UIIC			
7	Platform will not disclose or use any information and data generated such as user details, queries, responses, statistical data, and so forth, with any third party	M		
8	Solution shall support to enable/disable audit trail on specific data entities or transactions	M		
9	Solution shall generate audit trails for reports/queries executed	M		
10	The Solution shall protect the stored audit records from unauthorized deletion	M		
11	The Solution shall prevent modifications to the audit records	M		
12	Solution shall use encryption when transmitting passwords over the network	M		
13	Solution shall provide appropriate security at the RDBMS level to protect data from unauthorized personnel	M		
14	Solution shall support backup all data and metadata across all the sub systems of the proposed solution	M		
15	Solution shall provide mechanism for incremental and full backups with zero down time	M		
16	The solution shall prevent the display or printing of passwords	M		
17	The Solution shall provide the ability to provide an automatic log-off feature at user-specified time limits	M		
18	Solution shall manage all user credentials and permissions (eg: username, password) and user sessions	M		
19	Solution shall provide access to the system only using secured passwords and other identifiers as necessary	M		
20	Solution shall allow administer password policies such as minimum and maximum lengths, alphanumeric usage and expiry periods	M		
21	Solution shall provide users to change their passwords based on authentication rules	M		
22	Ability to provide read write, read only or execute level access to users based on role	M		
23	The solution maintains information on security events and can provide reporting on demand	M		
24	Solution shall support advanced encryption standards (128 bit) for routing financial transactions and customer data through IVRS	M		

25	Solution shall route transactions over secured HTTPS, SSL channels	M		

Privacy & Consent Management

SNO	Requirement Description	Requirement Classification (M/E/O)	Bidder Response (Y/N)	Remarks
1	Clear data handling policies: Develop and follow guidelines for agents on how to handle customer data, ensuring data privacy and protection	M		
2	Consent management: Implement mechanisms to record and track customer consent for data processing, as required by applicable regulations	M		

Physical Security

SNO	Requirement Description	Requirement Classification (M/E/O)	Bidder Response (Y/N)	Remarks
1	Secure workstations: Ensure workstations are locked when not in use and equipped with privacy screens	M		

Network Security

SNO	Requirement Description	Requirement Classification (M/E/O)	Bidder Response (Y/N)	Remarks
1	Firewall protection: Integrate with firewalls as applicable to monitor and control incoming and outgoing network traffic	M		
2	Software Installation: Prevent use/installation of unauthorized software	M		

Compliance/Regulatory Requirement

SNO	Requirement Description	Requirement Classification (M/E/O)	Bidder Response (Y/N)	Remarks
1	Data protection regulations: Ensure compliance with relevant data protection regulations, such as the DPDP 2023, by implementing appropriate security measures and privacy practices	M		
2	Compliance : Adapting ISO 27001 security practices or any other security practices	M		

Security Assessment

SNO	Requirement Description	Requirement Classification (M/E/O)	Bidder Response (Y/N)	Remarks
1	Periodic Assessment: Conduct comprehensive security testing, including penetration testing and vulnerability scanning, configuration review, server compliance and other security assessments for Application, API, etc on periodic basis to identify and address potential vulnerabilities	M		

Employee Training & Awareness

SNO	Requirement Description	Requirement Classification (M/E/O)	Bidder Response (Y/N)	Remarks
1	Security training: Provide comprehensive training to employees on data protection, privacy regulations, and best practices for handling sensitive customer information	M		
2	Incident reporting: Encourage employees to report security incidents promptly and establish procedures for incident response	M		
3	Agreement: Non-disclosure agreement signed by the agents during onboarding should contain details for formal disciplinary action procedures	M		

Application Security

SNO	Requirement Description	Requirement Classification (M/E/O)	Bidder Response (Y/N)	Remarks
1	User names and passwords must be hashed or encrypted at storage as well as before passing them over the network for authentication purpose Hashing should confirm to at least SHA2+Salt as well as strong crypto algorithm must be used which are not deprecated/ demonstrated to be insecure/ vulnerable	M		
2	Application should provide role based authorization which should be enforced through proper session management or privilege check for every action	M		
3	The proposed solution should be able to log 1) All actions taken by any individual with root or administrative privileges 2) Access to all audit trails 3) All elevation of privileges 4) All changes, additions, or deletions to any account with root or administrative privileges	M		
4	Service provider shall conduct security testing for applications, all plugins and web services planned/ exposed for Web Server	M		

I/We hereby state that the above information is true, and we have gone through the document and we undertake that we have understood all the requirements

I/We hereby agree to abide by all the IT security guidelines to the satisfaction of UNITED INDIA INSURANCE COMPANY

Yours faithfully,

For:

Signature & Seal:

Name:

Designation:

Date & Location: