Ref: 000100/HO IT/RFP/664/2025-2026

Annexure 18 - IT & IS Annexure

Sr no	Area	Requirement Description	Bidder Response	Bidder Remarks
1	**Security Access Control**	Multi-factor authentication: Implement a strong authentication mechanism to verify the identity of platform user accessing the system		
2	**Security Access Control**	Role-based access controls: Define access privileges based on job roles to limit access to sensitive data only to authorized personnel		
3	**Security Access Control**	Password policies: Enforce strong password policies to ensure secure access to systems		
4	**Data Security**	Encryption in transit: Require the use of secure protocols (such as TLS1.3) to protect data transmitted between systems and endpoints		
5	**Data Security**	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		
6	**Data Security**	Data retention and disposal: Establish policies and procedures for retaining and disposing		
7	**Data Security**	Platform to ensure Sensitive information like AADHAAR number and other PII information to be masked or encrypted in the database		
8	**Data Security**	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		
9	**Data Security**	Bidder should comply with all the guidelines issued by IRDAI/DFS/DoT/TRAI/Govt of India, IT ACT, 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		
10	**Data Security**	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		
11	**Data Security**	Solution shall support to enable/disable audit trail on specific data entities or transactions		
12	**Data Security**	Solution shall generate audit trails for reports/queries executed		
13	**Data Security**	The Solution shall protect the stored audit records from unauthorized deletion		
14	**Data Security**	The Solution shall prevent modifications to the audit records		
15	**Data Security**	Solution shall use encryption when transmitting passwords over the network		
16	**Data Security**	Solution shall provide appropriate security at the RDBMS level to protect data from unauthorized personnel		
17	**Data Security**	Solution shall support backup all data and metadata across all the sub systems of the proposed solution		
18	**Data Security**	Solution shall provide mechanism for incremental and full backups with zero down time		
19	**Data Security**	The solution shall prevent the display or printing of passwords		
20	**Data Security**	The Solution shall provide the ability to provide an automatic log-off feature at user-specified time limits		
21	**Data Security**	Solution shall manage all user credentials and permissions (eg: user name, password) and user sessions		
22	**Data Security**	Solution shall provide access to the system only using secured passwords and other identifiers as necessary		
23	**Data Security**	Solution shall allow administer password policies such as minimum and maximum lengths, alphanumeric usage and expiry periods		
24	**Data Security**	Solution shall provide users to change their passwords based on authentication rules		
25	**Data Security**	Ability to provide read write, read only or execute level access to users based on role		
26	**Data Security**	The solution maintains information on security events and can provide reporting on demand		
27	**Data Security**	Solution shall support advanced encryption standards (256 bit) for routing financial transactions and PII/Customer data		
28	**Data Security**	Solution shall route transactions over secured HTTPS, SSL channels		
29	**Privacy & Consent Management**	Clear data handling policies: Develop and follow guidelines for the platform on how to handle customer data, ensuring data privacy and protection		
30	**Privacy & Consent Management**	Consent management: Implement mechanisms to record and track customer consent for data processing, as required by applicable regulations (including DPDP guidelines as applicable)		
31	**Physical Security**	Secure workstations: Ensure workstations are locked when not in use and equipped with privacy screens		
32	**Network Security**	Firewall protection: Employ firewalls to monitor and control incoming and outgoing network traffic		
33	**Network Security**	Intrusion Detection and Prevention Systems (IDPS): Implement IDPS to detect and prevent unauthorized access or attacks		
34	**Network Security**	Secure Wi-Fi: Use encryption protocols (such as WPA2) and strong passwords for wireless networks		
35	**Network Security**	Software Installation: Prevent use/installation of unauthorized software		
36	**Compliance/Regulatory Requirement**	Data protection regulations: Ensure compliance with relevant data protection regulations, such as the DPDP 2023 or revisions thereof, by implementing appropriate security measures and privacy practices		
37	**Compliance/Regulatory Requirement**	Compliance : Adapting ISO 27001 security practices or any other security practices		
38	**Security Assessment**	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		
39	**Employee Training & Awareness**	Security training: Provide comprehensive training to employees on data protection, privacy regulations, and best practices for handling sensitive customer information		
40	**Employee Training & Awareness**	Incident reporting: Encourage employees to report security incidents promptly and establish procedures for incident response		
41	**Application Security**	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		
42	**Application Security**	Application should provide role based authorization which should be enforced through proper session management or privilege check for every action		
43	**Application Security**	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		
44	**Application Security**	Service provider shall conduct security testing for applications, all plugins and web services planned/ exposed for Web Server		

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: