Revised Annexure F: Technical and Functional Requirements

All the requested services in the scope are to be provided by the bidder. All the clauses which are Mandatory ('M') are to be complied for successful qualification.

#	Technical Specifications	Mandatory (M)/ Non-Mandatory (NM)	Evidence (with page no. of the document)	Compliance	Remark
1	The solution must support up to 500 Windows endpoints	M			
2	The solution must be deployed in On-prem	M			
3	Solution must support high availability and disaster recovery functions	M			
4	The Systems must seamlessly integrate with Core System application and must support interface with other open-standard systems	M			
5	Solution must have capabilities to restrict viewing, restrict sharing of rights, restrict copy/paste, editing, restrict screenshots or print screen, ip restrictions etc.	M			
6	Solution must have capabilities of dynamic watermarking, password protection to the file, document expiry and other standard features	M			
7	Solution must have a central console for defining policy, creating groups of systems/users, logging, deploying updates, securing user credentials, role based access, restricting access to user, allowing change in application, ip based access, multi-factor authentication, email/SMS notifications	M			
8	The solution must have 24x7 OEM support	NM			
9	The Incident Management team support will be 8 x 5	M			
10	Must provide role-based access to the console to allow specific admins to carry out read/write/read & write as per permission	M			
11	The solution should have granular control of policy based on group/device/user	M			
12	The solution should have compatibility	M			

#	Technical Specifications	Mandatory (M)/ Non-Mandatory (NM)	Evidence (with page no. of the document)	Compliance	Remark
	of Scale-out when needed				
13	The solution should have built-in capabilities to collect logs locally on the endpoint for troubleshooting	M			
14	The solution must be compliant to DPDP Act, IRDAI and requirements of other regulatory bodies as applicable to LIC from time to time	M			
15	Console access should integrate with Active Directory (AD) or third-party authentication systems, enforcing Multi-Factor Authentication (MFA).	M			
16	Solution should prevent concurrent sessions of same user to enhance security	NM			
17	Solution must use modern and easy remote deployment/ installation/ uninstallation methods (Including script support)	M			
18	The solution must allow to manage the agent version and components from the management interface	NM			
19	The solution should be able to provide real-time email alerts	M			
20	The solution should be able to provide pre-defined and customized Reports and logs as per requirement for Audit, internal reporting and forensic analysis	M			
21	Solution should support all versions of Windows including 10, 11 and future versions	M			
22	Agent must be lightweight (With evidence - Low CPU and Memory Usage, Minimal Disk Footprint, Efficient Network Usage etc.)	NM			
23	Solution should be configurable for minimal system resource utilization	NM			
24	Solution should not impact or conflict with native built-in OS security controls or other enterprise security tools currently	NM			
25	The solution should have the capability of Content encryption and Watermarking	M			
26	The solution should have the capability of User authentication and	M			

#	Technical Specifications	Mandatory (M)/ Non-Mandatory (NM)	Evidence (with page no. of the document)	Compliance	Remark
	authorization to access the protected content and track user activity				
27	The solution should have the capability of content revocation in case of unauthorized access to content	M			
28	The solution should have the capability of allowing access based on role and user	M			
29	The solution should have the capability of restricting access to unauthorized user	M			
30	The solution should have the capability of role creation, deletion, and updation	M			
31	The solution should have the capability of putting password protection on the file	M			
32	The system shall provide support for HTTPS/SSL/TLS for secured data transfer	M			
33	The system shall support a web-based administration module for the complete management of the system	M			
34	The solution should have the capability to restrict the user to uninstall the endpoint agent	NM			
35	The solution should have the capability of creating rights protection policies on internal and external users	M			
36	The solution should ensure compatibility with existing endpoints, OS, and network infrastructure	M			
37	The solution package size should include only the relevant components for deploying in a single installer	NM			
38	The solution should be able to retrieve agent updates over the Intranet	M			
39	When performing upgrades, the solution should download only the accumulated changes from the installed version	NM			
40	The solution should have built-in capabilities to collect logs locally on the endpoint for troubleshooting	M			
41	Solution must allow for real-time alerting or logging of notable events	M			

#	Technical Specifications	Mandatory (M)/ Non-Mandatory (NM)	Evidence (with page no. of the document)	Compliance	Remark
	based on custom content (behaviours)				
42	User should be able to see his/her permissions on the document post download. The solution should have the ability to control the level of messages to show to users and control over document post download	M			
43	Solution must be able to immediately apply preventive controls (block specific activity)	M			
44	The solution must capture user activities and should be available for download for further processing.	M			
45	The solution should be able to capture user activity if the client is offline and doesn't have an internet connection	M			
46	The right protections enforced on any file should stay with the file while being transferred over any medium. (Email, USB, Web, etc).The solution should have capability to enforce right protection on out-going communication over Email, Web and External Media	M			
47	The solution must have Integration with DLP, Data classification, PIM/PAM, ITSAM, AD, LDAP etc.	M			
48	The solution should protect one or multiple files simultaneously on the Laptops/Desktops with ease of use - Right Click on a file/multiple files and enable protection	M			
49	User should be able to protect the documents when attached in the email	M			