Annexure F: Technical Compliance

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	Compliance	Remark
1	The solution must support up to 3,000 Windows endpoints and 1000 licenses for the in-scope applications integration.	M			
2	The solution must deploy in On-prem.	M			
3	Solution must support high availability and disaster recovery functions	M			
4	Solution must have a deeply functional and documented API to support integration and automation across the platform available	M			
5	The systems must seamlessly integrate with Core system Application and shall support interface with other open-standard systems	M			
6	Solution must have capabilities to restrict viewing, restrict sharing of rights, restrict copy/paste, editing, restrict screenshots or print screen, Ip & mac ID restrictions.	M			
7	Solution must have capabilities Dynamic watermarking, camera protection, password protection to the file, document expiry	M			
8	Solution must have a central console for defining policy, creating groups of systems/users, logging, deploying updates, Secure User Credentials, access as per role defined, restrict access to user, allow change in application, Ip and mac-based access, 2 factor authentication, email notifications	M			
9	The solution must have OEM support 24x7x365.	NM			
10	The Incident Management team support will be 8 x 5	M			
11	Must provide role-based access to the console to allow specific admins to	M			

#	Technical Specifications	Mandatory (M)/ Non-Mandatory (NM)	Evidence	Compliance	Remark
	carry out read/write/read & write as per permission				
12	Granular control of policy based on group/device/user.	M			
13	The solution should have compatibility of Scale-out when needed.	M			
14	DRM Solution should have built-in capabilities to collect logs locally on the endpoint for troubleshooting	M			
15	The solution must be compliant to DPDP Act, IRDAI and requirements of other regulatory bodies applicable to LIC	M			
16	Console access should support using 3rd party systems authentication (Two Factor Authentication)	M			
17	Solution must use provide 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 as per requirement for Audit and internal reporting	M			
21	Supported OS like Windows	M			
22	Agent must be lightweight. Present evidence of average CPU, memory, and disk use during different activities with the capabilities	NM			
23	Solution is configurable for minimal system resource utilization	NM			
24	Solution does 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 authorization to access the protected content and track user activity.	M			

#	Technical Specifications	Mandatory (M)/ Non-Mandatory (NM)	Evidence	Compliance	Remark
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 restrict 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 support provide support for HTTP/SSL 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 of encrypting the data transferring over email and web.	NM			
35	The solution should have the capability to restrict the user to uninstall the endpoint agent.	M			
36	The solution should have the capability of creating rights protection policies on internal and external users	M			
37	The DRM solution ensures compatibility with existing endpoints, OS, and network infrastructure.	M			
38	The solution package size will include only the relevant components for deploying in a single installer	NM			
39	The solution should be able to retrieve agent updates over the Intranet.	M			
40	When performing upgrades, the solution will download only the accumulated changes from the installed version	NM			
41	DRM Solution should have built-in capabilities to collect logs locally on the endpoint for troubleshooting.	M			

#	Technical Specifications	Mandatory (M)/ Non-Mandatory (NM)	Evidence	Compliance	Remark
42	Solution must allow for real-time alerting or logging of notable events based on custom content (behaviours)	M			
43	The solution should have the ability to control the level of messages to show to users and control over document post download	M			
44	Solution must be able to immediately apply preventive controls (block specific activity)	M			
45	DRM Solution must capture user activities and quickly pivot the same on protected data.	M			
46	The solution should be able to capture user activity if the client is offline and doesn't have an internet connection	M			
47	The solution will identify and put right protection out-going communication over email, web, and external media	M			
48	The solution must have Integration with DLP, Data classification, PIM/PAM,ITSAM, LDAP etc.	M			