Annexure F: Technical Compliance

All the requested services in the scope are to be provided by the bidder. 100% compliance is necessary for mandatory technical specifications provided below for successful qualification of the bidder.

Data Leakage Prevention (DLP)					
#	**Technical Specifications**	**Mandatory (M) / Non–Mandatory (NM)**	**Evidence**	**Compliance**	**Remarks**
1	The solution must support up to 5k endpoints/clients (Windows), 30K email users and 30K Web users	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 with the customer	M			
5	Solution must have a central console for defining policy, creating groups of systems/users, logging, deploying updates, reporting	M			
6	The solution must have OEM support 24x7x365.	M			
7	The Incident Management team support will be 8 X 5 (on-site).	M			
8	Must provide role-based access to the console to allow specific admins to carry out read/write/read & write as per permission	M			
9	Granular control of policy based on group/device/user.	M			
10	The solution should have compatibility of Scale-out when needed.	M			
11	The solution should be able to provide a remote collection of troubleshooting logs	M			
12	Solution must be GDPR, CCPA, DPDP, IRDAI compliant	M			
13	Console access should support using 3rd party authentication systems	M			
14	Solution must use provide modern and easy remote deployment/installation/uninstallation methods (Including script support) by GPO or SCCM.	M			
15	The solution must allow to manage the agent version and components from the management interface	M			
16	The solution should be able to provide real-time email alerts	M			
17	The solution should be able to provide pre-defined and	M			

Data Leakage Prevention (DLP)					
#	**Technical Specifications**	**Mandatory (M) / Non–Mandatory (NM)**	**Evidence**	**Compliance**	**Remarks**
	customized Reports as per requirement for Audit and internal reporting purpose				
18	Support Windows OS	M			
19	Agent must be lightweight with minimal CPU memory/disk usage during different activities.	M			
20	Solution does not impact or conflict with native built-in OS security controls or other enterprise security tools currently integrated with the Gold Load or standard Server builds	M			
21	The solution allows upgrade to newer versions with/without performing a reboot.	M			
22	The solution should have the capability of OCR techniques.	M			
23	The solution should have the capability of automation and incident response.	NM			
24	The solution should have the capability of protecting sensitive data while taking print screens/screenshots.	M			
25	The solution should have the capability of putting protective measures while sending sensitive information via Bluetooth	M			
26	The solution should have the capability of Intelligent data discovery by using latest techniques.	NM			
27	The solution must be able to capture data leakage over image files, zip files, etc.	M			
28	The solution should have the capability of encrypting the data transferring over external storage. It Should support both Native and Portable Encryption and manage the removable media Encryption and DLP policies from the same management Console.	NM			
29	The solution should have the capability to restrict the user to uninstall the endpoint agent.	M			
30	The solution should have the capability of creating policies by using Classifiers, File types, File size, Regular Expressions, Classified data, fingerprinted data etc.	M			
31	The endpoint solution must be compatible with both 32-bit and 64-bit Windows operating systems,	M			

Data Leakage Prevention (DLP)					
#	**Technical Specifications**	**Mandatory (M) / Non–Mandatory (NM)**	**Evidence**	**Compliance**	**Remarks**
	including Windows 8, Windows 8.1, and 10, as well as Windows Server 2016, and Windows Server 2019. It should also have the capability to support Email DLP in Microsoft Azure or on-premises 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				
32	The DLP solution ensures compatibility with existing endpoints, OS, and network infrastructure.	M			
33	The solution package size will include only the relevant components for deploying in a single installer	M			
34	The solution should be able to retrieve agent updates over the Internet/Intranet.	M			
35	Solution must continuously collect system events necessary for detection and analysis. Vendor must list specific items that are collected in real time	M			
36	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	M			
37	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.	NM			
38	Solution must capture detailed metadata around sensitive data content based on policy applicable on both files being shared within the network and going out of corporate networks on endpoints.	M			
39	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	M			

Data Leakage Prevention (DLP)					
#	**Technical Specifications**	**Mandatory (M) / Non–Mandatory (NM)**	**Evidence**	**Compliance**	**Remarks**
	performed on incidents, such as “Change Status” or comments added by admins.				
40	The solution should have the ability to control the level of messages to show to users	NM			
41	Solution must be able to immediately apply preventive controls (block specific activity)	M			
42	Solution must allow analysts the ability to quickly pivot between different activities observed on an endpoint and provide contextual information if available	M			
43	The solution should have support of multiple 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.	M			
44	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.	M			
45	The DLP solution should have capabilities to monitor and block sensitive data content for unauthorised applications	NM			
46	The solution will allow scheduled data discovery scanning of local drives and Network locations	M			
47	The solution will leverage advanced mechanism, latest techniques and rules to identify data leakage and apply preventive Controls.	M			
48	The solution will identify and block out-going communication over Email, web, and External Media.	M			
49	Solution will automatically create an incident analysis for every detection/prevention that occurs.	M			
50	Employ different fingerprinting methods to signify sensitive data.	M			
51	Capability to exert sufficient control on external devices being connected in the environment.	M			
52	Flexible reporting options for	M			

Data Leakage Prevention (DLP)					
#	**Technical Specifications**	**Mandatory (M) / Non–Mandatory (NM)**	**Evidence**	**Compliance**	**Remarks**
	technical as well as high level reports.				
53	Multiple deployment options comprising of Hardware and Software.	M			
54	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.	M			
55	The solution should provide a framework for the integration of the Data Loss Prevention (DLP) systems with Digital Right Management (DRM), Data classification, and CASB solutions.	M			
56	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.	M			
57	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.	M			
58	The solution should Provide “Cloud Storage Applications” group which monitor sensitive content accessed by any cloud storage application on the endpoint and prevent sensitive data from uploading to the cloud.	M			
59	The solution should Support PrtSc blocking on endpoint when configurable list of specific application are running, no matter it is in the foreground or background. The actual PrtSc capture will also be submitted to the DLP system as forensic evidence.	M			
60	The Endpoint DLP Solution must be able to encrypt data when business classified data is sent to	NM			

Data Leakage Prevention (DLP)					
#	**Technical Specifications**	**Mandatory (M) / Non–Mandatory (NM)**	**Evidence**	**Compliance**	**Remarks**
	removable media drives. The encryption solution should be inbuilt with DLP component and not dependent upon any 3rd party solution to meet the requirement.				
61	The solution should have a comprehensive list of pre-defined policies and templates with over support of multiple patterns to identify and classify information pertaining to different industries and India IT Act.	M			
62	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	M			
63	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.	M			
64	The solution should enforce policies to detect low and slow data leaks	NM			
65	The solution should be able to identify data leaked in the form unknown and known encrypted format like password protected word document	M			
66	The solution should have the capability to prepare customizable policies for identifying and blocking activities like data thefts, encrypted file formats, etc.	M			
67	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.	M			
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	M			
69	The incident should display the	M			

Data Leakage Prevention (DLP)					
#	**Technical Specifications**	**Mandatory (M) / Non–Mandatory (NM)**	**Evidence**	**Compliance**	**Remarks**
	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	M			
71	The solution should allow a specific incident manager to manage incidents of specific policy violation, specific user groups etc.	M			
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 identity 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	M			
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	M			
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.	M			
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.	M			

Data Leakage Prevention (DLP)					
#	**Technical Specifications**	**Mandatory (M) / Non–Mandatory (NM)**	**Evidence**	**Compliance**	**Remarks**
76	The system should allow reports to be mailed directly from the UI and should allow automatic schedule of reports to identified recipients	M			
77	The reports should be exported to at least CSV, PDF formats	M			
78	The system should provide options to save specific reports as favourites for Reuse	M			
79	The system should have lots of pre-defined reports which administrators can Leverage	M			
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.	NM			
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.	M			
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	NM			
83	The system should allow automatic movement or relocation of file, delete files during discovery	NM			
84	The system should display the original file location and policy match details for files found to violate policy	M			
85	The system should leave the "last accessed" attribute of scanned files unchanged so as not to disrupt enterprise backup processes	M			
86	The system should support	M			

Data Leakage Prevention (DLP)					
#	**Technical Specifications**	**Mandatory (M) / Non–Mandatory (NM)**	**Evidence**	**Compliance**	**Remarks**
	incremental scanning during discovery to reduce volumes of data to be scanned.				
87	The OEM should have own technical support centre in India.	M			
88	The OEM should be present in India for more than 10 years and large customer reference	M			
89	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.	M			
90	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	M			
91	The solution should support Email DLP in Microsoft exchange on prem for all users. All licenses required for the same should be included and management should be from the same centralized management platform	M			
92	The proposed solution should provide Incident Workflow capabilities where user/Business Manager can remediate the DLP policy violations actions from handsets/emails with or without logging into the Management Console	M			
93	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 latest techniques and technologies. Solution must support Rest API for policy management along import and export of policies as well	M			
94	Endpoint must support the following operations on sensitive data that your	M			

Data Leakage Prevention (DLP)					
#	**Technical Specifications**	**Mandatory (M) / Non–Mandatory (NM)**	**Evidence**	**Compliance**	**Remarks**
	DLP endpoint can address: • Copy and paste controls (i.e., clipboard activities) • Save content to different locations, including saving to: • Local folders • Remote file shares Saving to cloud storage locations				
95	Ability to seamlessly integrate with encryption and selectively encrypt data on the basis of designed policies	M			
96	Enforce compliance over data sitting in different locations and be able to remediate all the issues identified for ensuring compliance.	M			
97	Ability to handle data being written on different types of media and option to monitor or prevent the same	M			
98	Capability to monitor and block all the traffic flowing out of the network, irrespective of Policies being in place or not	M			
99	Quick Deployment capability and Single Management Console for configuring Uniform Policies across network	M			
100	The solution must detect/identify and block the following: - Password protected file - Encrypted file - Sensitive data sent over mail - Sensitive data uploaded over the web - Sensitive data copied to External storage (USB, HDD, Mobile Transfer) - Sensitive data while taking printouts NOTE: In case of any other channel LIC wants to add solution/OEM must support.	M			
101	The solution must have the ability to generate visual reports Solution must provide an agent and DLP Component's health status.	M			
102	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	M			

Data Leakage Prevention (DLP)					
#	**Technical Specifications**	**Mandatory (M) / Non–Mandatory (NM)**	**Evidence**	**Compliance**	**Remarks**
	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.				
103	The solution must have Integration with SIEM and other security solutions (DRM, Data classification, CASB, PIM/PAM, ITSM, AD/LDAP etc.)	M			
104	Solution must support data at rest scanning for Exchange, Outlook PST, Databases, SharePoint and File systems	M			
105	Solution must support SMB, NFS and CIFS for Windows and non-Windows based file shares	M			
106	Solution must support TCP or ICMP scan methods when searching network shares	M			
107	Network Data discovery tasks must have a scheduler option by: once, daily, weekly or continuously	M			
108	Network Data discovery task must support inclusion and exclusion by file type, folders, age or size	M			
109	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.	M			
110	Network Data discovery must have an option to preserve original access time	M			
111	Network Data discovery must support bandwidth allocation for discovery process scanning	M			
112	Proposed solution should be able to deploy agent using common software methods like GPO, SCCM, etc. Proposed solution should support integration with Active Directory LDAP	M			
113	Solution should allow 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.	M			
11	Solution should allow dynamic,	M			

Data Leakage Prevention (DLP)					
#	**Technical Specifications**	**Mandatory (M) / Non–Mandatory (NM)**	**Evidence**	**Compliance**	**Remarks**
4	real-time tuning of rules and policies & should provide hierarchical management of rules, including higher-level groupings that map to business objectives				
115	Solution should provide emergency offline based override of policies based of administrative password.	M			
116	Solution should allow powerful rule construction, using keywords and/or regular expressions in standard Boolean logic	M			
117	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.	M			

Data Classification (DC)					
#	**Technical Specifications**	**Mandatory/ Desirable**	**Evidence**	**Compliance**	**Remarks**
1	The solution must support up to 5k endpoints/clients (Windows).	M			
2	The solution must deploy in On-prem.	M			
3	The solution must have OEM support 24x7x365.	M			
4	The Incident Management team support will be 8 X 5 (on-site)	M			
5	Bidder has to provide detail of OEM Support - Authorized partner for minimum one year ,support for the solution and MAF/back-to-back support for all components	M			
6	The Data Classification software licenses should be perpetual/subscription based and in warranty during first year and covered under Annual technical support of OEM for next 4 years	M			
7	Proposed Solution should be an on-premises Data Classification Tool .Specify the name of the solution and OEM of the solution	M			
8	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	M			

Data Classification (DC)					
#	**Technical Specifications**	**Mandatory/ Desirable**	**Evidence**	**Compliance**	**Remarks**
9	The solution should be in High Availability at primary site and DR site	M			
10	Solution should be capable for configuring at DC and DR	M			
11	The solution should be able to switch to DR seamlessly	M			
12	The solution should provide high availability seamless DC-DR migrations and vice versa	M			
13	The solution should be completely on-premises solution	M			
14	The solution should support scalability to meet LIC's future requirements	M			
15	The solution should enable the classification should support all mainstream server, desktop ,mobile, tablet and laptop Operating Systems (OS), which include the following: Desktop /laptops -Windows 10,11, Server-Windows Server 2016 and above	M			
19	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.	M			
20	The solution should have the capability to integrate with LIC access control systems PAM and Active Directory, and to integrate with SIEM and to send logs	M			
21	The Solution should provide classification logs inside the classified file and at the centralized repository.	M			
22	The solution should be able to classify unstructured data, namely word/excel/PowerPoint/pdf documents and MS Outlook emails.	M			
23	The Solution should Support for Email Servers like 0365 ,Web Mail owa , Exchange server	M			
24	The solution should enable the classification of Word, Excel and PowerPoint documents from within Microsoft Office.	M			
25	The solution should apply meta data tagging for various file formats like document, excel, ppt, pdf, image files, text files etc.	M			
26	The solution should be capable of integrating with OpenOffice to classify documents being created	NM			

Data Classification (DC)					
#	**Technical Specifications**	**Mandatory/ Desirable**	**Evidence**	**Compliance**	**Remarks**
	with OpenOffice				
27	The solution should enable user can define different Classification labels like public, internal, confidential, restricted etc.	M			
28	The solution should be able to label the documents in Headers/Footers with a preselection capability for either header or footer or both.	M			
29	The solutions should be able to insert metadata tags in the documents and emails which can be read by DLP Solutions.	M			
30	The solution should be able to track initial classification and reclassification events at both document and central logging level.	M			
31	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.	M			
32	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.	M			
33	The solution should trigger classification for document on Save, Save As, Print etc. and should be configurable using a management mechanism.	M			
34	The solution should trigger classification based on send, reply, forward emails.	M			
35	The solution should provide automated, suggestive and manual classification capability	M			
36	The solution shall have capability to classify multiple documents in one go.	M			
37	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	M			
38	The solution should have capability to detect differential classification between an email and it's attachments and block the email from being sent	M			
39	The solution should detect unclassified documents attached in an email and block the user from	M			

Data Classification (DC)					
#	**Technical Specifications**	**Mandatory/ Desirable**	**Evidence**	**Compliance**	**Remarks**
	sending the email.				
40	The solutions should not restrict the number of classification levels required to be created.	M			
41	The solution should be capable to deploy and enforcing user based policies.	M			
42	The solution should be able to identify information like Aadhar, Passport numbers, credit card ,insurance policy information for automated classification thru either inbuilt capability or should have capability to define regular expressions.	M			
43	The solution should be able to detect keywords as defined by the organization and enforce classification	M			
44	The solution should further allow policies which are based on a combination of keywords and regular expressions.	M			
45	The solution should allow administrators to define own regex for adding capability to detect any new type of regex.	M			
46	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.	M			
47	The solution should log user activity while users are handling email, documents, and files.	M			
48	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.	M			
49	The solution should have Manual, Automated and Suggested Classification feature	M			
50	User can define different Classification labels like public, internal, confidential, restricted etc.	M			
51	User should be able to set default classification labels for each department	M			
52	Ability to classify based on content like if Credit card or Aadhaar card is identified, tool should automatically classify file as restricted	M			
53	Ability to customize visual marking, header, footer of word, excel, ppt etc.	M			

Data Classification (DC)					
#	**Technical Specifications**	**Mandatory/ Desirable**	**Evidence**	**Compliance**	**Remarks**
54	The solution should have Policy Configuration based on Departments and user groups from AD.	M			
55	The solution should have Print Protection: - Prevent user from printing sensitive files and emails.	M			
56	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.	M			
57	The solution should have ability for Auto classification files whenever user will download based on content or context	M			
58	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 it can be marked as confidential for business purpose while more than 5 it should be marked as restricted	M			
59	The solution should have Ability to prevent user from sending attachment without Classifying	M			
60	The solution should have Ability to automatically detect PII types in email body attachment and subject based on classification policy	M			
61	The solution should have Ability to prevent user from sending attachment with confidential or restricted content to outside domain based on policy	M			
62	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.	M			
63	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.	M			
64	The solution should Provide default classification department wise like if anyone from HR team has sent mail mark as internal for HR purpose.	M			
65	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 cannot.	M			
66	The solution should support	M			

Data Classification (DC)					
#	**Technical Specifications**	**Mandatory/ Desirable**	**Evidence**	**Compliance**	**Remarks**
	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.				
67	The solution should support icon overlays to identify the classification of files in File Explorer.	M			
68	The solution should provide tooltips, classification descriptions, and help page links to assist users with classification policy.	M			
69	The solution should support the creation of unlimited custom metadata for interoperability (Department, PII type, Document category, PII count etc.), including custom X-headers	M			
70	The solution should support customizable visual markings in email and documents (e.g. font (name/size/features), size, colour, and content).	M			
71	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.	NM			
72	The solution should provide the ability to attach metadata to information objects, which can be leveraged by DLP solutions.	M			
73	The solution should provide the ability to write tags which can be read by DLP solution	M			
74	The Solution should be managed via a centralized management console. The solution should have capability to manage the complete solution from a central Management Console	M			
75	The Management console should have role based access and should integrate with Active directory /LIC's Privilege Access Management system for login access	M			
76	The solution should provide built-in reports and dashboards to analyse user behaviour and system health.	M			
77	The solution should provide a pre-built starter set of reports for the reporting database (in Excel) and	M			

Data Classification (DC)					
#	**Technical Specifications**	**Mandatory/ Desirable**	**Evidence**	**Compliance**	**Remarks**
	Views and documentation to enable customers to write their own reports.				
78	The solution should provide a built-in dashboard for reviewing data classification scanning results for user activity, deployment.	M			
79	The solution should provide role based access for administrators, compliance teams where anyone other than administrators may not have access to full console.	M			
80	The solution should provide Customizable dashboard to create multiple dashboards based on user requirements.	M			
81	The solution should provide Dashboard to provide classification alerts based on timeframe	M			
82	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	M			
83	The solution should have a capability to deploy, upgrade, uninstall the agent with or without the use of any 3rd party software.	M			
84	The solution should be able to send policy and further changes to the clients without any need or intervention of a 3rd party software.	M			
85	The solution should have capability to deploy policies basis users, machines, groups etc.	M			
86	The unavailability of a management component/ server in no way shall impact the functioning of a client	M			
87	The solution should cache configurations locally for offline use.	M			
88	Ability to move systems from one group to other	M			
89	Ability to see the managed/unmanaged status of each system	M			
90	Ability to see last communication date and time of system with the Management server.	M			
91	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.	NM			
92	The solution should have Ability to add targets based on IP and hostname for dynamic environment	M			
93	The solution should have Support	M			

Data Classification (DC)					
#	**Technical Specifications**	**Mandatory/ Desirable**	**Evidence**	**Compliance**	**Remarks**
	various PII types like Aadhaar card, Pan Card, Driving license, National ID of different countries ,Policy numbers				
94	The solution should have Support for multiple privacy regulations like GDPR, DPDP, HIPAA, FIPS, IRDAI, etc.	M			
95	The solution should have Ability to tag files for classification for agent based and agent less discovery	M			
96	The solution should have latest technologies to identify images with Aadhaar Numbers, Credit cards, PAN Card, Password, Driving licenses of different states.	M			
97	The solution should have latest and advanced techniques where user can upload any kind of images and discover and classify similar kind of images	M			
98	The solution should have Scheduling automated scans without user intervention - daily, weekly, monthly, quarterly etc	M			
99	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.	M			
100	The solution should have Ability to identify sensitive data in data bases - which tables , which columns contains sensitive data	M			
101	The solution should have Ability to view the actual file data or table from the centralized console to validate the results easily	M			
102	The solution must have the capability to Discover, Classify and Protect the documents and emails without any user intervention	M			
103	The solution must have ability to assign classification level to discovered data elements according to policy	M			
104	The solution should be equipped with the ability to analyse and discover sensitive data, aligning with internal compliance requirements and regulatory guidelines	M			
105	The solution must have the capability to do analysis(discovering sensitive data)Based on file types (MS-office,	M			

Data Classification (DC)					
#	**Technical Specifications**	**Mandatory/ Desirable**	**Evidence**	**Compliance**	**Remarks**
	pdf's, TXT files, XML, HTML, JPEG, Compressed file's etc.)				
106	The solution must have the capability to do analysis(discovering sensitive data) along with host details	M			
107	The solution must have the capability to do analysis(discovering sensitive data) based on Current Classification Level and to suggest classification.	M			
108	The solution must have the capability to Delete/move/replace the sensitive data as a Remediation action if required.	M			
109	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	M			
110	The solution should provide Dashboard to provide discovery overview like how many targets completed scans every quarter vs not completed, Remediation taken etc.	M			
111	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.	M			
112	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	M			
113	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.	M			
114	The solution should provide Auto update features for agents. Admin should be able to push to the agents automatically after every release	NM			