RFP for Supply, Implementation, and Maintenance of Data Classification and Discovery Tool

RFP Ref : LIC/CO/IT-BPR/DCT/2023-24 Dated: 24.05.2023

Annexure VII A – revised:Functional and Technical Requirements

(In case bidder's response to any of the questions given below is "No",to a Mandatory question the bidder will be treated as disqualified for the bid)

Sr No	Functional and Technical Requirements	Mandatory(M)/ Non Mandatory(N)	Whether Available (Yes/No)	Bidder's Comments	Ref Page No.	Marks
	General					
1	Hardware components proposed in the Solution should preferably be enterprise class (Servers, Load Balancers, Switches, Storage etc.). Relevant Documentation to be submitted.	M				
2	The bidder should bring in the required Hardware ,load balancer, rack network equipment etc for the solution .Sizing should take into consideration successful running of the solution for period of 5 years . Item wise Bill of material of hardware and software components to be provided by bidder	M				
3	The hardware component of solution should be under warranty for 3 years and AMC for 2 years with back to back support from OEM .The selected bidder shall guarantee a Monthly uptime of minimum 99.90% for the Backend Infrastructure (hardware/software from the date of commencement of the proposed solution.	M				
4	Bidder to provide details of implementation team along with appropriate experience in implementation of similar solutions	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 and Data Discovery 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				
	Data Classification and Data discovery Tool solution -					
7	Proposed Solution should be an on premises Data Classification Tool and Data Discovery solution .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				
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				
	The solution should enable the classification should support all mainstream server, desktop ,mobile, tablet and laptop Operating Systems (OS), which include the following					
15	Desktop /laptops -Windows 10,11	M				
16	Desktops-RHEL 7.* and above versions with Open office ,pdf files	M				
17	Server-Windows Server 2012 and above	M				
18	Server -RHEL 7.* and above with web server/application server	M				
19	Server-SUSE Linux	M				
20	Server -IBM Linux, IBM AIX, HPUX, Solaris	N				
	The solution should enable the classification should support the following					
21	Open office with base OS RHEL	M				
22	MS Office 2007 onward versions ,pdf files ,Support for scanning all types of file formats like pdf, excel, ppt, word, text files, files without extensions.	M				
23	Support for Email Servers like 0365 ,Web Mail ,owa , Exchange server, MS Outlook and Thunderbird (*LIC requires support for Exchange on premises . O365 is for future and Point is Non Mandatory*)	M N for O365				
24	Support for Cloud Environment like AWS S3, Azure, Google Cloud	M				
	The solution should enable the discovery of sensitive data and classification on and should support following DB and file servers					
25	DB-MySQL with base OS -RHEL	M				
26	DB-Oracle with base OS RHEL	M				
27	DB-Oracle-exadata ,with base OS oracle linux(engineered system)	M				
28	DB-SAP HANA DB Server and MS SQL server	M				

29	DB-Vertica and DB-Email Server-Exchange	M				
30	File Server -Windows OS, Sharepoint (on premise)	M				
31	File Server on cloud -SharePoint-online ,OneDrive and Box.	N				
32	File Server on base OS RHEL	M				
33	Document Management System(Omnidocs) -Scanned Documents	M				
34	Support for scanning all types of file formats like pdf, excel, ppt, word, text files, files without extensions	M				
35	Support to scan compressed files like zip, rar, 7z etc	M				
36	Support for scanning Image files with OCR	M				
37	Support for scanning images inside PDF, Document, PPT etc.,CAD -engineering drawings CAD files support is Non mandatory	M				
38	Support for scanning Audio Files	N				
39	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	M				
40	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				
41	The Solution should provide classification logs inside the classified file and at the centralized repository.	M				
	Classification Features					
42	The solution should be able to classify unstructured data, namely word/excel/PowerPoint/pdf documents and MS Outlook emails.	M				
43	The solution should enable the classification of Word, Excel and PowerPoint documents from within Microsoft Office.	M				
44	The solution should apply meta data tagging for various file formats like document, excel, ppt, pdf, image files, text files etc.	M				
45	The solution shall have capability to send emails from mobile with classification applied for both IOS and Android based mobiles.	N				
46	The solution should be capable of integrating with OpenOffice to classify documents being created with OpenOffice.	M				
47	The solution should enable user can define different Classification labels like public, internal, confidential, restricted etc.	M				

48	The solution should be able to label the documents in Headers/Footers with a preselection capability for either header or footer or both.	M				
49	The solutions should be able to insert metadata tags in the documents and emails which can be read by DLP Solutions.	M				
50	The solution should be able to track initial classification and reclassification events at both document and central logging level.	M				
51	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				
52	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				
53	The solution should trigger classification for document on Save, Save As, Print etc. and should be configurable using a management mechanism.	M				
54	The solution should trigger classification based on send, reply, forward emails.	M				
55	The solution should provide automated, suggestive and manual classification capability	M				
56	The solution shall have capability to classify multiple documents in one go.	M				
57	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				
58	The solution should have capability to detect differential classification between an email and it's attachments and block the email from being sent	M				
59	The solution should detect unclassified documents attached in an email and block the user from sending the email.	M				
60	The solutions should not restrict the number of classification levels required to be created.	M				
61	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	M				
62	The solution should be capable to deploy and enforcing user based policies.	M				

63	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.	M				
64	The solution should be able to detect keywords as defined by the organization and enforce classification	M				
65	The solution should further allow policies which are based on a combination of keywords and regular expressions.	M				
66	The solution should allow administrators to define own regex for adding capability to detect any new type of regex.	M				
67	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				
68	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.	N				
69	The solution should log user activity while users are handling email, documents, and files.	M				
70	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				
71	The solution should have Manual, Automated and Suggested Classification feature	M				
72	User can define different Classification labels like public, internal, confidential, restricted etc.	M				
73	User should be able to set default classification labels for each department	M				
74	Ability to classify based on content like if Credit card or Aadhaar card is identified, tool should automatically classify file as restricted	M				
75	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				
76	Ability to customize visual marking, header, footer of word, excel, ppt etc.	M				
77	The solution should have Policy Configuration based on Departments and user groups from AD.	M				
78	The solution should have Print Protection: - Prevent user from printing sensitive files and emails.	M				

79	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				
80	The solution should have ability for Auto classification files whenever user will download based on content or context	M				
81	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	M				
82	The solution should have Ability to prevent user from sending attachment without classifying	M				
83	The solution should have Ability to automatically detect PII types in email body attachment and subject based on classification policy	M				
84	The solution should have Ability to prevent user from sending attachment with confidential or restricted content to outside domain based on policy	N				
85	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				
86	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				
87	The solution should Provide default classification department wise like if anyone from HR team has sent mail mark as internal for HR purpose.	M				
88	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.	M				
89	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.	M				
90	The solution should support icon overlays to identify the classification of files in File Explorer.	M				
91	The solution should provide tooltips, classification descriptions, and help page links to assist users with classification policy.	M				
92	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				

93	The solution should support customizable visual markings in email and documents (e.g. font (name/size/features), size, colour, and content).	M				
94	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.	M				
95	The solution should provide the ability to attach metadata to information objects, which can be leveraged by e-discovery solutions.	M				
96	The solution should provide the ability to write tags which can be read by DLP solution	M				
	Data Discovery					
97	The solution should generate metadata for all file types, including persistent, embedded metadata for many non-Office files, including PDF, Visio, Project, images, and multimedia files.	M				
98	The solution should have Remediation Options like Truncate, Mask/Redact, Delete for files and	M				
99	The solution should have Data Discovery for file shared for both SMB and NTFS protocol	M				
100	The solution should have The solution should have Quarantine/ Safe Folder to move sensitive data stored in an un-protected location to a secure location	M				
101	The solution should have ability of Quarantine encryption of files to local folders	M				
102	The solution should have Ability to discover host in a network along with OS details and multiple targets with domain name, keys or passwords.	M				
103	The solution should have Ability to upload /scan targets in bulk from excel files.	M				
104	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	M				
105	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.	M				
106	The solution should have Ability to to discover systems using IP range and add targets based on IP and hostname for dynamic environment	M				
107	The solution should have Support various PII types like Aadhaars card, Pan Card, Driving license, National ID of different countries ,Policy numbers	M				
108	The solution should have Support for multiple privacy regulations like Indian Data Protection(Draft bill) etc. mandatorily and preferably for GDPR, CCPA, LGPD,	M				

109	The solution should have Ability to tag files for for classification for agent based and agent less discovery	M				
110	The solution should have AI/ML capability to reduce false positives	M				
111	The solution should have Pre trained AI models to identify images with Aadhaars Numbers, Credit cards , PAN Card, Password, Driving licenses of different states.	M				
112	The solution should have Self Trained AI Model where user can upload any kind of images and discover and classify simillar kind of images	M				
113	The solution should haveScheduling automated scans with out user intervention - daily, weekly, monthly, quarterly etc	M				
114	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				
115	The solution should have Ability to identify sensitive data in data bases - which tables , which columns contains sensitive data	M				
116	The solution should have Ability to view the actual file data or table from the centralized console to validate the results easily	M				
117	The solution must have the capability to Discover, Classify and Protect the documents and emails without any user intervention	M				
118	The solution must have ability to assign classification level to discovered data elements according to policy	M				
119	The solution must have the capability to do analysis(discovering sensitive data) Based on Compliance requirement (PII, PHI, etc.)	M				
120	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.)	M				
121	The solution must have the capability to do analysis(discovering sensitive data) along with host details.	M				
122	The solution must have the capability to do analysis(discovering sensitive data) based on Current Classification Level and to suggest classification.	M				
123	The solution must have the capability to do analysis(discovering sensitive data) along with the User Permission on the sensitive data.	M				
124	The solution must have the capability to Delete the sensitive data as a Remediation action if required.	M				
125	The solution must have the capability to move the sensitive data as a Remediation action if required.	M				
126	The solution must have the capability to replace the sensitive data as a Remediation action if required.	M				

	Dashboard & Reporting					
127	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				
128	The Management console should have role based access and should integrate with Active directory /LIC's Privilege Access Management system for login access	M				
129	The solution should provide built-in reports and dashboards to analyse user behaviour and system health.	M				
130	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.	M				
131	The solution should provide a built-in dashboard for reviewing data classification scanning results for user activity, deployment.	M				
132	The solution should provide role based access for administrators, compliance teams where anyone other than administrators may not have access to full console.	M				
133	The solution should provide Customizable dashboard to create multiple dashboards based on user requirements.	M				
134	The solution should provide Dashboard to provide discovery overview like how many targets completed scans every quarter vs not completed, Remediation taken etc.	M				
135	The solution should provide Dashboard to provide classification alerts based on timeframe	M				
136	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				
	Deployment, Installation & Updates					
137	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.	M				
138	The solution should provide Easy deployment of agents with support of Active Directory	M				
139	The solution should have a capability to deploy, upgrade, uninstall the component without the use of any 3rd party software	M				
140	The solution should provideMinimal impact for end points . User should be able to choose low, medium and high usage for agents	M				
141	The solution should provide Auto update features for agents. User should be able to push the agents automatically after every release.	M				

142	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				
143	The solution should have capability to deploy policies basis users, machines, groups etc.	M				
144	The unavailability of a management component/ server in no way shall impact the functioning of a client	M				
145	The solution should cache configurations locally for offline use.	M				
146	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				
147	Protection Controls like Restrict user to send the email in case specific software like AV, FW etc are not running on the user's systems	N				
148	Ability to move systems from one group to other	M				
149	Ability to see the managed/unmanaged status of each system	M				
150	Ability to see last communication date and time of system with the Management server.	M				
	Total 150 marks ,minimum required marks is 70% of 150 =105 and all mandatory points should be complied .Compliance should be demonstrated in presentation/demo/POC					
	Note: Available carry one mark and Not available carry zero mark.					
	Declaration: We hereby confirm that the information submitted above is true to the best of our knowledge. We understand that in case any discrepancy is found in the information submitted by us our tender is liable to be rejected.					
	Date Signature with seal:					
	Name : Designation:					

RFP for Supply, Implementation, and Maintenance Data Classification and Data Discovery Tool
RFP Ref : LIC/CO/IT-BPR/DCT/2023-24 Dated: 24.05.2023

Annexure VII – B- revised: Technical Capability Criteria

	Technical Capability Criteria			
		Points		
S No	**Criterion**	**Item**	**Value**	**Marks**
1	Average annual revenue for the last 3 Financial Years(Eligibility Criteria(EC) Rs 60 Cr ;	**revenue(>500 Cr)**	**15**	
		revenue(151-500 Cr)	**10**	
		revenue(60-150 Cr)	**5**	
2	Partnership of bidder with proposed Data Classification and Data Discovery tool Solution OEM minimum 1year ;	**> 5yr**	**15**	
		> 1 to 4.9 yrs	**10**	
		1 year	**5**	
3	Total implementation (1000 users from minimum 1 implementations in India;	**> 5000 to 10000 users and 4 and above implementations**	**15**	
		> 1000 to 5000 users and 2 to 3 implementations	**10**	
		1000 users and 1 implementation	**5**	
4	Installed Data Classification and Data Discovery tool Count(in a Single Installation)	**>25000 to 50000**	**15**	
		>10000 to 25000	**10**	
		10000	**5**	
5	Availability of employees certified by OEM/having security related certification and experienced in implementing the proposed solution (list with names /qualifications to be provided)	**> 25**	**15**	
		>15 to 25	**10**	
		5 to 15	**5**	

6	Experience in Security Practice especially in Data Flow mapping	**4 and above implementations**	**15**	
		2 to 3 implementations	**10**	
		1 implementation	**5**	
7	The bidder having experience in implementation and maintenance the proposed Data Classification Tool	**> 7yr**	**10**	
		> 3 to 6.9 yrs	**5**	
		1 to 3 yr	**2.5**	
	Total Marks 100 ,Minimum marks required is 70% of 100 =70 marks			
	Marks Scored by bidder in VIIB Technical scoring criteria			