Terms of Reference

Supply, Implementation, Commissioning and Maintenance of Data Classification & Data Leakage Prevention Solution SMIB/TD/2025/10/02

1. **Background.**

State Mortgage and Investment Bank (SMIB) hereby invites Expressions of Interest (EOI) from qualified and experienced consultants for the supply, implementation, commissioning, and maintenance of a Data Classification and Data Leakage Prevention (DLP) Solution. The engagement will span a period of three (03) years, in accordance with the terms and conditions specified in the project documentation.

SMIB intends to deploy a comprehensive Data Classification and DLP solution across endpoints, network, and email systems at selected locations. The objective is to prevent the leakage of confidential data and customer information, thereby mitigating corporate risk associated with both unintentional and intentional disclosure of sensitive information. This initiative aligns with SMIB's commitment to data control and regulatory compliance.

The DLP solution will be centrally managed and monitored from a location designated by SMIB, primarily the Head Office, and must incorporate adequate redundancy to ensure high availability and reliability.

The primary goal of the project is to successfully implement and maintain a robust Data Classification and DLP solution. The implementation will be phased, initially covering 100 endpoints, and subsequently expanding to a total of 300 endpoints. The selected consultant will be responsible for the installation, configuration, support, and ongoing maintenance of the solution. Furthermore, the consultant will serve as the single point of contact for all matters related to the solution, including documentation, training, and technical guidance.

2. Project Scope

2.1 General Scope

The Consultants who wish to take up the project shall be responsible for the following:

2.1.1 To classify the data and deploy the DLP solution adequately sized and scalable Software, Applications, Tools, Utilities, related Services and Facilities Management as per Specifications, terms and conditions and scope defined in this RFP.

2.1.2 Consultant must maintain all involved application/database level components required for the proposed solution. In case, if Consultant is supplying the customized

OS, then the Consultant has to take care of OS level installation, configuration, support and its further maintenance as well.

2.1.3 Rollout the proposed solution covering all the SMIB identified locations as specified under the given scope.

2.1.4 Impart Training and Knowledge Management to the SMIB's management and personnel.

2.1.5 Provide Facilities Management Services for the implemented solutions.

2.1.6 Provide complete hand-over along with detailed documentation on at the end / termination of the UAT acceptance (First and Second Phase of the project).

2.1.7 The key personnel(s) identified for the project should carry out their activities from SMIB's premises if needed.

2.2 Broad Scope of Work

2.2.1 The Consultant shall be responsible for analyzing the requirements and proposing a comprehensive solution, inclusive of a data classification framework, which shall be fully aligned with SMIB's existing policies and procedures. The proposed solution shall be designed to integrate seamlessly with SMIB's current systems, network, and security infrastructure, ensuring full compatibility. In the event that SMIB undertakes a revamp of its architecture or migrates to an alternative network technology or location, the Consultant shall, at no additional cost to SMIB, implement all necessary modifications to the solution to ensure uninterrupted functionality and successful adaptation to the new deployment environment.

2.2.2 The Consultant is required to supply the Software/Licenses/Applications required to provide above solutions at DC, DRC & Branches and other SMIB locations, as applicable. The solutions shall comply with the requirements provided in the document –Technical specifications & Broad Scope of work.

2.2.3 The Consultant must ensure that quoted Software should not be end of sale within 5 years of supply to SMIB. Consultant shall also ensure that no component is declared either End of Support, End of Life during tenure of the contract. In case the consultant/ OEM (Original Equipment Manufacturer) fails to give the above data for any specific component, and later on, any specific component is found to have date of end of sale/ support/ life which falls before the end date of the contract the consultant will have to replace / upgrade the component free of cost with the latest workable component.

2.2.4 Consultant is required to make available required resources that may be required for the successful completion of the entire assignment within the quoted cost to SMIB.

2.2.5 The proposed Data Classification & DLP solution should be scalable to support up to 300 Endpoints during the tenure of the contract.

2.2.6 The software shall be provided with a comprehensive three (03) year onsite warranty, commencing upon successful completion of the User Acceptance Testing (UAT).

2.2.7 SMIB reserves the right to bring about any changes in Requirement/Scope of this RFP and the same will be communicated to the consultant well in time so as to allow the consultant to prepare their proposal.

2.2.8 The selected consultant is responsible for arranging for the prompt, conclusive & secure closure of any vulnerability pointed out in any of the security Reviewer, IT Audits carried by SMIB or SMIB appointed third party or any issues/bug/concerns in the proposed solution. If the Issue requires OEMs (Original Equipment Manufacturers/Software Owners) technical person's product developer etc. intervention, selected consultant has to take up suitability with the appropriate Level at OEM and obtain the solution and implement it for resolution of the issue. If the analysis of the issue requires log submission, Consultant will submit the same for further analysis in consultation with SMIB.

2.2.9 The Consultant shall be responsible for the following:

2.2.9.1 Procurement of the necessary solutions and the corresponding software, database etc. required for implementing these solutions at SMIB.

2.2.9.2 Implementation of the identified solutions at SMIB including configuration, customization & Integration of the products as per the requirement. Also, implemented solution must meet SMIB's system security requirements.

2.2.9.3 Consultant to specify the need of VM or other hardware for storage or hosting of application in their technical bid. (SMIB will provide the necessary Hardware, bidder shall mentioned the required specifications on Bill of materials)

2.2.9.4 The consultant shall provide the detailed technical architecture comprising of hardware (including configuration) with operating systems and other application software in their technical bid.

2.2.9.5 In case the consultant has not indicated any peripherals /equipment in their proposed solution and if same is required for successful implementation of proposed solution then cost of those components should be borne by the consultant.

2.2.9.6 Consultant shall apply all software updates / version upgrades released by the respective OEMs during the contract period.

2.2.10 The consultant may propose best feasible architecture at the time of technical bid submission, which is cost effective, takes care of high availability, adequate redundancy and fault tolerance to ensure compliance with SLAs for uptime, in case DC setup fails and during DR drill as well.

2.2.11 The proposed solution should be capable of covering all, but not limited to, the following:

a. Endpoints
b. Email Server

2.2.12 All software offered is required to be licensed to the SMIB. Consultant is required to size all the hardware/software for the solution proposed.

2.2.13 Consultant shall also undertake to carry out implementation / operationalization including move, add and delete, changes / customization of such hardware & software updates, releases, version upgrades. Implemented solution must meet the SMIB's prevailing standards.

2.2.14 Consultant has to configure the rules/policies in the proposed solution. Consultant can also fine-tune such policies/rules in case if requires.

Manpower Support required during working days schedule as below:

Location	**Expected Experience and Level of Support**	**Time**	**Number of Resources**
SMIB Head Office / Branches	**3 to 7 years of experience and L2 Support**	**Resources in Shift 1 (Monday to Saturday*) Starting 8.00 AM to 4.30 PM**	**1**

2.2.15 Vendor shall provide onsite support on all SMIB working days at SMIB Head Office, branches or any other place SMIB requested as mentioned above shift schedule for post go live maintenance/support. The support shall start from the date of successful implementation and acceptance of the solution by the SMIB. The onsite support person should be well versed with the solution with adequate experience. In case the performance of the support Person is not satisfactory, the person should be replaced upon SMIB’s request. Onsite support person should also be supporting DR Drill/Cyber Drill activities as and when scheduled by SMIB.

3 Technical Specifications

S. No.	General Requirements
1	The solution and services in scope should be built with sufficient redundancy and fault tolerance [Necessary hardware will be provided and replication tolls will be provided by SMIB]
2	The solution should not have a substantial impact on the current infrastructure during installation or operation.
3	The system should allow for central management of incidents that arise from email, endpoints, network, and discovery
4	The solution should be able to block or quarantine outbound emails sent via O365 SMTP if it violates the policy without an agent
5	The suggested solution should act as a Mail Transfer Agent, receiving emails from the mail server and inspecting the content before forwarding them to the next hop (mail gateway), as well as quarantining emails that violate business policy, all of which should be accomplished on the same solution
6	All essential licenses should be included, and administration should be done through the same centralized management platform
Endpoint Data Monitoring and Protection	
7	Even if the solution is away from the corporate network, it should be able to monitor data transferred to network file shares and apply structured and unstructured fingerprint policies.
8	In addition to blocking of external devises should have capability whitelist and blacklist of external devises (DLP policy activated). Information copied to removable media should be encrypted by the endpoint solution. It should enable both native and portable encryption, and it should be possible to administer encryption and DLP policies from the same console.
9	Endpoint solutions should support 64-bit operating systems, as well as a wide range of platforms.
10	Endpoint agent should have possibility to log and shadow all copied to USB files, printed files, copied to File Share and sent over the network files [Necessary storages will be provided by SMIB].
11	Endpoint TCP inspection should work without using a separate plugin.
12	System should be able to create separate set of rules for USB and File-Share channels.
13	System should be able to restrict usage of Bluetooth network cards.
14	System should inform security office in case of new USB inserted into the employee PC.
15	Agent should have possibility to restrict file copy to the USB device based on QTY of the files or QTY of information in Mb. This rule should block file copy after limit is reached for specified time
16	Agent should have possibility to block MTP/PTP protocol usage for employees.

17	The proposed solution should allow off-premises DLP prevention possibility at least for printers.
18	Agent should have possibility to work in stealth mode.
19	Agent should have possibility to work in tamper proof mode.
20	System should be able to enable screen watermark for user
Data Identification and Policy management	
21	A thorough collection of pre-defined policies, templates, and patterns for identifying and classifying information should be included in the solution
22	The solution should be able to identify data using keywords or patterns, as well as enforce restrictions based on file kinds, file sizes, and file names.
23	The solution should be able to detect and take action on encrypted and password-protected files without reading the encrypted content
24	The solution should be able to perform a full binary fingerprint on files as well as identify partial information leakage from fingerprinted files or directories; fingerprint hash should be minimum 64bits
25	The solution should be able to analyze compressed archive content in a recursive manner
26	The solution should be able to fingerprint just specified fields or columns inside a database and identify information from databases by correlating data in distinct columns.
27	The solution should be able to identify and prevent data leaks through the print channel.
28	The solution should enact measures to identify data breaches that are small and sluggish.
29	HTTP, HTTPS, SSH, RDP, SMTP, SCP, FTP, SFTP, and Webmail should all be intercepted by the endpoint agent
30	The solution should be able to identify Optical Character Recognition (OCR) in real-time
31	The solution should be able to enforce regulations to identify data breaches even in picture files via email channels using OCR technology
32	Based on the user's Incident patterns, the solution should be able to generate risk rankings.
33	The proposed DLP solution must be GDPR and PDPA compliant, with specific Personal Identifiable Information (PII).
34	OCR should build in inside the components of the solution not a separate server.
35	OCR should be applicable for all three: data in use, data in motion and data at rest. It should work for endpoint agent for all features: network interception, USB interception, Printing etc.
36	Agent should be able to intercept and apply OCR inspection for printed through Adobe Acrobat images in pdf format
Automated Response and Incident Management	
37	When a policy violation occurs, the solution should be able to alert and inform the sender, sender's manager, and policy owner. Different communication templates for different audiences should be allowed
38	The solution should offer quarantine as a response to email policy violations
39	The incident should include a clear indication of how the transmission or file violated policy (rather than just which policy was violated), as well as a

	clear identification of which content triggered the match, and the ability to open the original attachment directly from the user interface
40	For all network and endpoint channels, the incident should indicate the sender's complete identity (full name, department, manager name, etc.) as well as the transmission destination. In addition, the system should allow events to be assigned to single incident management
41	When a new incident is assigned to incident management, the solution should send them an automated notice, and the incident should not be deleted by anybody, even the product administrator
42	The system should enable a dedicated incident manager to handle problems involving particular policy breaches, user groups, and so on
Role-Based Access and Privacy Control	
43	Incident access should be controlled by the system based on the role and policy that was violated. The system should also allow for the creation of a role that does not have access to the user's identity or the incident's forensics.
44	For data at rest, in motion, or at the endpoint, the system should define different roles for technical management of servers, user administration, policy formulation and amendment incident remedy, and incident viewing
45	The system should allow users to define roles that allow them to view summary reports, trend reports, and high-level data but not individual events
46	The system should allow incident managers and administrators to log into the console using their Active Directory credentials
47	Two factor authentication should be supported for login to Console
Reporting and Analytics	
48	The solution should have a dashboard view for executives that combines data in motion (network), data at rest (storage), and data at the endpoint into a unified view
49	The system should allow reports to be emailed directly from the user interface, as well as an automated report schedule for certain recipients
50	The system should have a large number of pre-built reports that administrators may use.
Storage (data at rest)	
51	During data discovery scans, the proposed solution should enable automated file moving or relocation to a predefined location. File deletion should also be supported if necessary
52	For files discovered to be in violation of policy, the system should report the original file location as well as policy match information
53	To limit the amount of data to be scanned, the system should provide incremental scanning during discovery
Supports Third part recognitions	
54	The vendor must provide extensive hands-on training on how to operate the technology provided
55	The solution should be able to transmit user logs to a SIEM
Data Classification	

56	The solution must conduct Real-Time Data Classification on data in motion and at rest while also enforcing data security regulations automatically.
57	Proposed solution to offer both classification and Data Loss Prevention (DLP) features (preferably through a single agent – please mention)
59	The solution should be able to force user to classify and classification based on content
60	When documents and emails are first produced, the solution should label them. Existing documents in data repositories must be scanned for sensitive information. On-premise data storage should be used; categorized and labelled according to a Data Classification Policy that has been agreed
61	Documents should be labelled with visual markings such as watermarks, headers, and footers as part of the solution. Electronically marking the files will be required
62	System should prevent print screen action for classified Microsoft Office and PDF documents
63	Solution should control file copy operation block it or log, based on the classification of the File for Microsoft Office and PDF documents.
64	The solution should be able to track policy warnings and violations and provide options for reporting through email, or console view.
65	The solution must be able to generate on-demand, daily, weekly, and trending reports that indicate all policy breaches and warnings, as well as trending over time. The reports should include an examination of automatically categorized papers as well as a historical perspective of all document
66	The system should have auditing tools to verify that documents are categorized accurately and consistently in the future
67	The solution should have real time classification possibility after file is created, modified, downloaded, copied system should apply classification based on content
68	The vendor will be in charge of the solution's deployment and support, as well as trainings for system administrators. By presenting a chart or graphic, the vendor should give a complete project plan of the activities necessary in the implementation process, including all tasks, milestones, and deadlines.
69	The solution should be able to search for certain keywords and regular expressions and classify them appropriately.
70	The solution should allow users to customize visual markers in emails and documents (e.g. font, size, color, and content)
71	The solution should allow for real-time automated file categorization when files are downloaded and saved to certain folders (e.g. Downloads, My Documents, Desktop), with classification based on file content, file type, file size, file name, file path, and any combination of these criteria
72	The solution should classify printed documents
73	The solution should restrict sending of classified emails only to specific domains. Example: top secret email can be sent only within @test.com domain
74	The solution should be able to scan and classify specific files with a minimum effort such as a right click.
75	The solution should be able to classify images based on the content.

Information Protection	
76	The solution should have the ability to check for external recipients who have been designated in an email and alert/prevent the user from sending the email. For example, if external recipients are marked in an email containing an internally classified document as an attachment, the email should not be delivered. An alert should be sent to the user as well
77	The solution should allow users to be warned or prevented from downgrading or altering their categorization.
78	The solution should have the ability to downgrade, upgrade, and alter classification only for particular users and AD groups
79	The solution should allow for the restriction of email based on the sender. For example, one user may be allowed to transfer critical information outside the company, while others are not. The sender's email, name, AD characteristics, or group membership may be used to make the policy choice
80	The system should allow for policy combinations to enable more sophisticated use cases, such as determining whether a document contains regulatory data and then preventing an unauthorized user from transmitting the document as an attachment through email
81	For MS Outlook, the solution should have the option to prevent users from sending non-classified email attachments (i.e. attachments that have no classification)
Data Discovery	
82	The solution should support the discovery and identification of large volumes of data, stored both on-premise and cloud. This includes the scanning of network file shares as well as cloud storage providers
83	Data repositories should be scanned by DLP network discovery to find sensitive data at rest, such as local file systems on Windows, Linux, and other servers; NAS Storage; Microsoft, Outlook, Onedrive
84	The solution should allow administrators to create policies that include or exclude categorization.
85	The solution should be able to move critical files from unsecured storage directories to safe storage folders automatically.
86	The solution should allow for the collection of file information, such as file attributes, classification (pre- and post-scan), and access controls, during scans. This data inventory establishes the nature of the data, its location, and who has access to it.
87	The solution should be able to actively monitor file shares in real-time, with the capacity to perform actions like logging, copying, moving, deleting, and classifying files newly created, modified, downloaded, or copied within the shared folders.
Auditing and Reporting	
88	Depending on the situation, the solution should be able to deliver user logs to SIEM, Syslog server.
89	A built-in dashboard for analyzing data discovery scanning findings for user activity, deployment, data storage trends, and data inventory should be included in the solution.
90	Built-in reports and dashboards should be available to assess user activity.
91	The proposed solution should include an audit log to track opened, deleted, and modified documents within shared locations.

Configuration and Deployment	
92	For categorization configuration and policy maintenance, the system should provide a centralized, web-based Administration Console.
93	System administrator should have built-in update and uninstallation mechanism without use of 3rd party tools or Microsoft AD group policies.
94	System should have automated update scheduled search.
95	The solution should be able to directly interface with Active Directory (AD), enforcing restrictions based on AD groups and allowing administrators to customize configurations for individual users or groups of users
96	The solution should function with current versions of Windows OS, and the manufacturer should guarantee compatibility with future Windows OS releases.
97	The solution should work within virtual machine environments including VMWare, and other virtual desktop technologies.
98	System should have possibility to create custom groups without AD integration.

4 Project Locations

The selected bidder should supply DLP solution related software at:

i. Primary site: SMIB, No. 269, Galle Road, Colombo 03, Sri Lanka.
ii. Disaster Recovery Site: No. 49, Yakkala road, Gampaha
iii. All the SMIB Branchers

The workstations included within the scope of this project are currently deployed across various branch offices. SMIB reserves the right to modify the project location as deemed necessary to meet operational requirements.

5 Project Timelines

The selected bidder shall submit a comprehensive implementation schedule for the DLP solution, covering the full scope of the project. This schedule shall be reviewed and discussed with SMIB officials to reach a mutually agreed timeline, which must fall within a maximum duration of 32 weeks from the date of issuance of the Purchase Order (P.O.). The bidder shall be contractually bound to adhere to the agreed timelines across all three proposed phases of the project.

Phase One

Job	**Projected Timeline**
Study the existing policies, procedures of SMIB and applicable laws and regulations.	Within 2 weeks from the date of PO
Development of Data classification framework**.**	Within 4 weeks from the date of PO
Training of all SMIB Staff to Classify the data based on the developed framework.	Within 6 weeks from the date of PO
Review and validate the data classified by the SMIB staff and completion of data classification.	Within 12 weeks from the date of PO

Phase Two

Job	**Projected Timeline**
Software supply and installation	Within 2 weeks from the completion of phase one.
License Activation of first 100 nodes	Within 3 weeks from the completion of phase one.
Implementation (UAT) signoff	Within 4 weeks from the completion of phase one.
Rule configuration and endpoint rollout	Within 8 weeks from the completion of phase one.
Final Sign off and Start of Facilities Management (FM) services	Within 10 weeks from the completion of phase one.

Phase Three

Job	**Projected Timeline**
Installation agent software on 100 nodes	Within 1 week from the completion of phase two.
License Activation of 100 nodes	Within 1 week from the completion of phase two.
Implementation (UAT) signoff	Within 1 week from the completion of phase two.
Rule configuration and endpoint rollout	Within 4 weeks from the completion of phase two.
Final Sign off and Start of Facilities Management (FM) services	Within 5 weeks from the completion of phase two.

Phase Four

Job	**Projected Timeline**
Installation agent software on 100 nodes	Within 1 week from the completion of phase three.
License Activation of 100 nodes	Within 1 week from the completion of phase three.
Implementation (UAT) signoff	Within 2 week from the completion of phase three.
Rule configuration and endpoint rollout	Within 4 weeks from the completion of phase three.
Final Sign off and Start of Facilities Management (FM) services	Within 5 weeks from the completion of phase three.

6 PAYMENT TERMS

The payment will be released on completion of the job. SMIB will release the payment within 6 – 8 weeks of receiving the undisputed invoice, after deduction of applicable taxes at source of the agreed price to the selected Bidder. No advance payments will be made. All payments will be made on successful completion of the job to the satisfaction of SMIB and achievement of the objective as defined in the scope of work.

Phase One

Pay-out (% Cost)	**Milestone (Phase One)**
30	Sign-off of the Data Classification Framework
70	Completion of Data Classification

Phase Two

Pay-out (% Cost)	**Milestone (Phase One)**
20	Supply / Delivery of Solution
20	Successful installation, Configuration and acceptance
60	Licenses activation (**100 license only**), Final Sign off and Start of Facilities Management (FM) services and Successful running of the Solution for 1 month

Phase Three

Pay-out (% Cost)	**Milestone (Phase One)**
100%	License Activation (**100 license only**) Final Sign off and Start of Facilities Management (FM) services.

Phase Four

Pay-out (% Cost)	**Milestone (Phase One)**
100%	License Activation (**100 license only**), Final Sign off and Start of Facilities Management (FM) services.

7 Service Levels

Service level after implementation for operations & maintenance

Bidder need to strictly adhere to Service Level Agreement (SLA) computed on parameters as per industry best practice. Services delivered by vendor should comply with the SLA mentioned in the table below. SLA will be calculated on a monthly basis. SLA violation will attract penalties.

Service Area	Acceptable Service Level	Penalty
DLP Solution's Uptime % calculated on monthly basis for DLP solution. In case of any hardware problems, the Bidder should ensure that replacement devices are made available to meet the SLAs.	System Availability 99.9 % and above	NA
	98% to 99.8	2 % of monthly AMC payment of year 1 AMC
	95% to 97.99%	3 % of monthly AMC payment of year 1 AMC
	90% to 94.99%	5 % of monthly AMC payment of year 1 AMC
	85% to 89.99%	7 % of monthly AMC payment of year 1 AMC

8 Qualification criteria

Key Consultant	**Qualifications**	**Experience**
Project Manager	B.Sc. in IT or related and Relevant Industry Certifications	Minimum 3 years of experience as a project manager in DLP project management.
Classification Configuration Engineer	M.Sc. in IT or related and Relevant Industry Certifications	Minimum 3 years of experience in similar work
GRC Manager	B.Sc. in IT or related and Relevant Industry Certifications	Minimum 3 years of experience in similar work
Implementation Engineer	B.Sc. in IT or related and Relevant Industry Certifications	Minimum 2 years of experience in similar projects
Network Security Engineer	B.Sc. in IT or related and Relevant Industry Certifications	Minimum 2 years of experience in similar projects
Support Engineer	B.Sc. in IT or related and Relevant Industry Certifications	Minimum 2 years of experience in similar projects