## Scope of Work:

| Sl No | Description | Complied Yes/No | If No, Bidder's Remarks |
|---|---|---|---|
| 1 | The proposed solution should be deployable in inline as well as in listening mode. | | |
| 2 | The proposed solution should be able to block/alert pdf content access /Cut/Copy by image writer or by application like screen capturing /session recording tools etc. | | |
| 3 | The proposed solution should have wide range of out of the box rule sets | | |
| 4 | The proposed solution should support the following for rules creation and updation | | |
| | a. centralized console for rule creation and updation | | |
| | b. Ability to whitelist legitimate data format | | |
| | c. Ability to create custom rule set and apply it on select IP addresses/email IDs / directory groups etc. | | |
| 5 | The proposed solution should also capture violations made by users to defined policies when they are out of the Bank's network. | | |
| 6 | The proposed solution should provide SSL decryption and destination awareness capability on the gateway to identify any sensitive content uploading to online web properties, even when it is tunnel over SSL | | |
| 7 | The solution should have pre-defined applications and application groups and allow each application/application group to monitor operations like Cut/Copy, Paste, File Access and Screen Capture and also can add the custom applications. | | |
| 8 | The proposed solution must have the mechanism to index and retain all documents by monitoring all traffic policy rules. | | |
| 9 | The proposed solution should be able to perform following searches: | | |
| | a. e-mail sent from or to any email address | | |
| | b. traffic sent across protocols or ports | | |
| | c. Documents leaving the network based on document type/ document properties | | |
| 10 | The proposed solution should support : | | |
| | a. Scanning file formats such as (Word, excel, ppt, xls) | | |
| | b. Non textual pds, xps | | |
| | c. data in archival tools (.zip/rar/.7z/.tar). Alert presence of encrypted archived files | | |

| Sl No | Description | Complied Yes/No | If No, Bidder's Remarks |
|---|---|---|---|
| | d. analyze encrypted data over web proxies | | |
| | e. analyze data sent over email (organizational/non organizational - Gmail etc), mobile devices. | | |
| 11 | The proposed solution should be able to monitor IM Traffic even if it is tunnelled over HTTP protocol, and FTP traffic including fully correlating transferred file data with control information | | |
| 12 | The proposed solution should be able to prevent content getting posted or uploaded to specific geo-location. | | |
| 13 | The proposed 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. | | |
| 14 | The proposed solution should create an incident in the central management server or ticketing tool for all low, medium and critical or high level impacts | | |
| 15 | The proposed solution should be able to discover and identify sensitive information stored on endpoints, databases, file shares, sharepoint, SAN, NAS etc. | | |
| 16 | The proposed solution should have a mechanism to highlight any deviation from bank policies for storage of sensitive information | | |
| 17 | The proposed solution should be able to deploy both pattern matching and document tagging with 3rd party and fingerprinting | | |
| 18 | The proposed solution should be able to schedule periodically recurring scans to identify sensitive data at rest | | |
| 19 | The proposed solution should have the capability to encrypt the sensitive content when copied. | | |
| 20 | The proposed solution should Encrypt data transferred to portable media with encryption of 256 bit and above | | |
| 21 | The proposed solution should be able to monitor movement of sensitive data at endpoint through various channels such as bus, Bluetooth, LPT etc. | | |
| 22 | The proposed solution should be able to inspect documents embedded in other documents | | |
| 23 | The proposed solution should be able to track the copying of data into USB drives, media cards and mobile phones if they considered as removable media. | | |
| 24 | The proposed Solution should notify the end user of a policy violation using a customizable pop-up message and should capture content that violates a policy and store it in an evidence repository | | |

| Sl No | Description | Complied Yes/No | If No, Bidder's Remarks |
|---|---|---|---|
| 25 | The proposed solution should control access to USB based on various parameters such as designation of individuals | | |
| 26 | The proposed solution should restrict access to sensitive data based on user roles. | | |
| 27 | The proposed solution should restrict sensitive information from being printed | | |
| 28 | The proposed Solution should be able to enforce policies for thick and thin clients | | |
| 29 | The proposed solution should allow encryption of complete hard drive sector by sector | | |
| 30 | The proposed solution should be able to configure policies to detect on fingerprints and files from share/repository/date created etc. | | |
| 31 | The proposed solution should enforce policies to detect and prevent low and slow data leaks. | | |
| 32 | The proposed solution should have a comprehensive list of pre-defined policies and templates to identify and classify information pertaining to Banking industry / India IT Act/DPDP Act. | | |
| 33 | The proposed solution should be able to enforce policies to detect and prevent data leaks even on image files | | |
| 34 | The proposed solution should have a dashboard view. | | |
| 35 | The proposed solution should support reports in different formats such as PDF, Excel or CSV, etc. format. | | |
| 36 | The proposed solution should allow Karnataka Gramin Bank and Kerala Gramin Bank to develop reports built around stakeholder requirements such as top policy violations, senders, content type, protocol and historical reports etc. | | |
| 37 | The proposed solution should support the following type of analysis | | |
| | a. Regular expression/pattern matching/indexing/tags etc. | | |
| | b. Based on file names. | | |
| | c. Full text/ URL requested. | | |
| | d. Should have the capability to check with full/partial documents. | | |
| | e. Should be able to provide information on how many times a user has violated DLP policies | | |
| 38 | The proposed solution should support the following for analysis | | |
| | a. Capture the metadata for further inspection | | |
| | b. Capture SMTP headers, from and destination IP addresses, date/time etc. | | |

| Sl No | Description | Complied Yes/No | If No, Bidder's Remarks |
|---|---|---|---|
| 39 | The proposed solution should provide an ability to perform full scans and incremental scans | | |
| 40 | The proposed solution should have options to see summary reports, trend reports and high-level metrics etc. | | |
| 41 | The proposed solution should have a mechanism for incidents to be sorted by severity level, sender, recipient, source, destination, protocol and content type etc. | | |
| 42 | The proposed solution should be able to alert and notify sender, sender's manager and the policy owner whenever there is a policy violation, different notification templates for different audience should be provided | | |
| 43 | The proposed solution should support quarantine as an action for email policy violations and should allow the sender's manager to review. | | |
| 44 | 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 UI | | |
| 45 | The proposed solution should trigger only one incident per event, even if the event violates multiple policies. | | |
| 46 | The proposed solution should have a mechanism to support easily downloadable upgrades from OEM official website | | |
| 47 | The proposed solution should be able to generate the monthly report which is required for analysis of endpoint DLP performance. | | |

## Technical Specifications of Endpoint Data Loss Prevention Solution

| Sl No | Features | Complied (Yes/No) | If No Bidders Remarks |
|---|---|---|---|
| **Information Protection: Data Loss Prevention** | | | |
| **Data Loss Prevention - Policies** | | | |
| 1 | Ability to choose from comprehensive list of pre-defined policies, templates and also should support customization of the same. | | |
| 2 | Ability to monitor and protect data classifiers created in via the Fingerprinting of documents. | | |
| 3 | Capability to identify data based on keywords or dictionaries and the solution should be able to enforce policies based on file types, file extension, etc. | | |
| 4 | Able to detect and alert password protected files | | |
| 5 | Proposed solution should designate individual (or groups of) removable devices as trusted and create policy exceptions for those devices. | | |
| 6 | Ability to govern and restrict sensitive data transfer over Teams chats and channel message, including file transfers and also should support for other media channel transfer. | | |
| 7 | Should be able to detect and prevent:<br>- Keywords/patterns and proximity to each other within documents<br>- Pre-built dictionaries<br>- Wide range of sensitive data types (e.g., Aadhar,PAN, SSNs, CCNs etc.)<br>- Patterns with respect to various compliances like PCI-DSS, GDPR etc.<br>- Classified Proprietary File types (types that are not predefined)<br>- Content in images (for example JPEG, PNG etc.) using Optical Character Recognition (OCR).<br>- File copied to cloud domains<br>- File printed<br>- Copy to clipboard<br>- Copy to removable storage<br>- copy to network share can be blocked<br>- Copy to bluetooth<br>- Copy over RDP<br>- User creates an item<br>- User renames an item<br>- data uploaded by unallowed browsers<br>- Data accessed by unallowed apps | | |

| Sl No | Features | Complied (Yes/No) | If No Bidders Remarks |
|---|---|---|---|
| 8 | Shows a policy tip and sends an email notification to users when they attempt to share protected sensitive information with people outside/inside your organization. | | |
| 9 | Allow automatic movement of files with policy violations and replace with a message from admins. | | |
| 10 | Extends DLP capabilities to items that are used and shared on Windows 10, Windows 11 and higher versions and macOS (Catalina 10.15 and higher) devices. | | |
| 11 | Should have the ability to store and index the capture event data with appropriate metadata (date/time, user, protocol etc.). | | |
| 12 | Evidence collection for file activities on devices. | | |
| 13 | Solution should Index and retain all unfiltered files that are analyzed while scanning files. | | |
| 14 | Ability to detect the web uploads over the blocked web domains. | | |
| 15 | Ability to customize action rules, including email notification, blocking, quarantining, redirection, bouncing etc. | | |
| 16 | Ability to provide an option of policy/rule override in case a business requirement dictates data transfer and notification to be sent to the admin. | | |
| 17 | Ability to define a single set of policies based on content, sender/recipient, file characteristics and communications protocols once and deploy across all products. | | |
| 18 | Ability to search across all captured data, across all workloads during investigations and incident response workflows. | | |
| **DLP: Centralized Management** | | | |
| 1 | Configurations and control of all scanning should be possible from the single, centralized console. | | |
| 2 | Unified policy enforcement platform. | | |
| 3 | The central Management console should have a built-in Agent health status dashboard. | | |
| 4 | The solution should support the onboarding and management of devices using the DLP console. | | |
| 5 | The solution should keep track of all incidents and should provide an option to close the incident after providing the remarks and the report should be available for audit. | | |

| Sl No | Features | Complied (Yes/No) | If No Bidders Remarks |
|---|---|---|---|
| **DLP: END USER NOTIFICATIONS** | | | |
| 1 | Automatic email notification should be sent to user and/or reporting authority upon the generation of an incident. | | |
| 2 | Ability to send emails for approvals to sender's manager or an approving authority before sending sensitive data out via email. | | |
| 3 | Policy violation should be captured in activities and should also be sent to admins via emails. | | |
| 4 | Alerts generated must have a severity level that is configured while creating the policies | | |
| 5 | Notification should be automatic displayed to educate users of potential policy violations. | | |
| 6 | Option for endpoint user self-remediation (on-screen notification prompting user to confirm whether to continue or cancel confidential data transfer). | | |
| 7 | Ability to notify the end user of a policy violation using a customizable pop-up message with hyperlinks and fields for user justification and should capture content that violates a policy and store it in an evidence repository. | | |
| **DLP: Policy Definition** | | | |
| 1 | Define policies based on content, sender/recipient, file characteristics, and communications protocol | | |
| 2 | Configure policies to detect/set thresholds based on number of matches on a per policy basis | | |
| 3 | Provide pre-defined policy templates based on India and international regulations and corporate best practices that can be customized | | |
| 4 | Create policies that combine multiple rules with AND/OR logic and exception rules | | |
| 5 | Define group-based detection rules based on internal directory information, such as department or business unit | | |
| 6 | Enable a single policy to combine multiple detection techniques | | |
| 7 | Directory based policies to selectively monitor downloads based on user, business units, or directory groups | | |