DHANLAXMI BANK LIMITED
CORPORATE OFFICE,
PUNKUNNAM, THRISSUR - 680002

REQUEST FOR PROPOSAL

Data Leakage Prevention & Data Classification Solution

RFP No: DLB_ISG/ RFP/ 2022-23/001

6th May 2022

Prepared by

Information Security Group

RFP Details in Brief

RFP No. and date	RFP No: DLB_ISG/ RFP/ 2022-23/001
Brief Description of the RFP	Request for Proposal for Data Leakage Prevention and Data Classification Solution
Bank's Address for Communication	Information Security Group 3rd Floor, Corporate Office Dhanlaxmi Bank Punkunnam, Thrissur Kerala - 680002
e-mail for Submission of Tender	ciso@dhanbank.co.in
Contact Details	Ms.Seetha Vimal ISG Department 3rd Floor, Corporate Office Dhanlaxmi Bank Punkunnam, Thrissur, Kerala - 680002 Ph: +91 487 7107336 e-mail:seetha.vimal@dhanbank.co.in
Date of Issue	06/05/2022
Last date of submission of any queries, clarifications etc.	13/05/2022
Last Date of submission of RFP response as soft copy	20/05/2022

DISCLAIMER

The information contained in this Request for Proposal ("RFP Document") or information provided subsequently to bidder(s) or applicants whether verbally or in documentary form by or on behalf of Dhanlaxmi Bank Limited, is provided to the bidder(s) on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided.

This RFP document is not an agreement and is neither an offer. The purpose of this RFP is to provide applicants who are qualified to submit the bids ("Bidders") with information to assist them in formulation of their proposals ("Bids") This RFP does not claim to contain all the information each Bidder may require. Each Bidder may conduct its own independent investigations and analysis and is free to check the accuracy, reliability and completeness of the information in this RFP. Bank makes no representation or warranty, express or implied, and shall incur no liability whatsoever under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFP. Bank may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP.

The information contained in the RFP document is selective and is subject to update, expansion, revision and amendment. Dhanlaxmi Bank does not undertake to provide any Bidder with access to any additional information or to update the information in this RFP or to correct any inaccuracies therein, which may become apparent. Dhanlaxmi Bank reserves the right of discretion to change, modify, add to or alters any or all of the provisions of this RFP and/or the bidding process, without assigning any reasons whatsoever. Such change will be intimated or made accessible to all Bidders. Any information contained in this document will be superseded by any later written information on the same subject made available/accessible to all recipients by Dhanlaxmi Bank.

Information provided in this RFP is on a wide range of matters, some of which may depend upon interpretation of law. The information given is not intended to be an exhaustive account of statutory requirements and should not be regarded as a complete or authoritative statement of law. Dhanlaxmi Bank does not own any responsibility for the accuracy or otherwise for any interpretation or opinion on law expressed herein. Further, Dhanlaxmi Bank also does not accept liability of any nature whether resulting from negligence or otherwise howsoever caused arising from reliance of any Bidder upon the statements contained in this RFP

Dhanlaxmi Bank reserves the right to reject any or all the responses to RFPs/Bids received in response to this RFP at any stage without assigning any reason whatsoever and without being liable for any loss/injury that Bidder might suffer due to such reason. The decision of

Dhanlaxmi Bank shall be final, conclusive and binding an all the parties directly or indirectly connected with the bidding process.

It may be noted that notice regarding corrigenda, addendums, amendments, time-extensions, clarifications, response to bidders' queries etc., if any to RFP, will not be published through any advertisement in newspapers or any other media. Prospective bidders shall regularly visit Bank's website for any changes / development in relation to this RFP.

Contents

1. INTRODUCTION

Incorporated in November 1927, Dhanlaxmi Bank (here in after known as "DLB") headquartered at Thrissur in Kerala, became a Scheduled Commercial Bank in the year 1977. DLB is currently having 520 touch points spread across India including branches, ATMs and BCs, which are connected by MPLS. Most of these locations are connected with more than one MPLS link from different service providers and network routing established with BGP. Branch locations are having the bandwidth capacity from 256 Kbps to 2Mbps depending upon the size of the particular branch and bandwidth availability.

Bank has also implemented Security Operation Centre (SOC) and integrated the servers / devices for log analysis and monitoring of servers / devices installed across the bank network.

DLB has state of the art Data Centre (DC) hosted at Nxtra Data Ltd (Bharthi Data Centre Managed Services) Bangalore and Disaster Recovery (DR) site at ContrlS, Hyderabad. DLB has implemented Flexcube Core Banking Solution (CBS) in all the branches in India.

To further strengthen the IT Infrastructure, Bank has already got accreditations from International Certifying Authority like BSI (ISO: 27001) for the IT and IT related operations of the bank.

2. REQUIREMENT

Dhanlaxmi Bank is on the verge of implementing a well-designed Data Protection strategy and robust security framework. To ensure monitoring and control over sensitive data, reduce the impact of any potential data leakage and ensure security of its infrastructure, DLB intends to engage with OEMs / partners / Bidders to recommend and deploy a suitable Email Data Leakage Prevention (DLP) platform, and a Data Classification platform, to monitor approximately 2500 email users across 245 branches of DLB, PAN India. Further services of this partner / bidder are to support implementation and rollout of email DLP and also provide the optional resource cost for extending Data Leakage monitoring and Incident management services. The Bidder should note that:

a) The technical specifications specified in the Evaluation excel sheet are the minimum specifications for the solution.

b) The purpose behind issuing this RFP is to invite pre-qualification, technical and commercial bids from the eligible bidders and selection of bidder(s) for the above purpose.

c) The selection process consists of the following three phases:

- ✓ Pre-Qualification/Minimum Eligibility Criteria
- ✓ Technical Evaluation
- ✓ Commercial Evaluation

Dhanlaxmi Bank invites bids (Technical bid and Commercial bid) from eligible bidders as per requirements mentioned in the RFP. The invitation of Bids is open to all Original Equipment Manufacturers (OEMs) having presence in India or their Authorized

Representative in India, provided bidders fulfill the minimum qualification criteria as mentioned in bid document. Please note that any deviations mentioned in the bid will not be considered and evaluated by the Bank. Bank reserve the right to reject the bid, if bid is not submitted in proper format as per RFP.

3. SCOPE OF WORK

The bidder will be expected to provide Data Leakage Prevention solution covering Email as well as a solution for Data Classification.

3.1 General Requirements

- The bidder shall be responsible to build, manage and operate the solution, i.e. implementation, data classification, departmental interlock, build policies and handle other operational activities – policy fine tuning, monitoring & manage incident management desk.
- The Vendor shall assign a project leader and associated support personnel for this project.
- Vendor shall assign appropriate resources with fairly rich experience to Build and Implement DLP solutions and among them -
    - ✓ One resource with 2-3 years of experience in DLP technology to Manage and operate post sign off for evaluating false positives and false negatives; fine tune the data protection policies to correct the errors. Review overall feedback and exceptions.
- The proposed solution shall have extensive Reporting, dashboards and auditing capabilities.
- Support the solution including future upgrades of all components of the solution, without any exception for a minimum period of 3 years from the date of go live (Extendable for another 2 years upon Bank's discretion)
- Support for application version / hardware-cum-software infrastructure.
- Provide the details of the architecture of the proposed solution containing complete details of specifications of components of proposed solution
- Solution must Safeguard employee privacy – balancing the needs of corporate data protection along with the need for employee privacy
- Visibility and control over data including:
    - ✓ Encrypted data;
    - ✓ Image files etc.
- Summarize the similar incidents, Incident workflow and case management.
- Role based administration for internal administrative tasks, monitoring and enforcement.
- Ensure no unwarranted, illegal, and fraudulent misuse of data shared by Bank.
- Bidder to categorically indemnify Bank against any losses that Bank may suffer on account of any such fraudulent and illegal act by the Company or its employees.

- Solution should provide for built-in/predefined policies/templates for BFSI and geographies, and can be accessed, used, and applied simultaneously for solution that provides content, context and destination awareness, allowing administrators to manage who can send what information, where and how.
- The proposed DLP solution should block, quarantine or relocate the channel containing sensitive data.
- Define Key performance indicators (KPI), which are aligned with overall data protection strategy, such as number of data leakage incidents, network coverage, Rules configured, reduction of false positives, Incidents closed within SLAs etc.
- Perform Configuration of Policies: Provide assistance to configure the tool with required rules.
- Full documentation of the project is to be included in the deliverables by the successful Vendor.

3.2 Implementation of DLP with Email gateway

- The solution should provide the central management for the incidents generated over Email, and discovery.
- The solution should be able to block outbound emails sent via SMTP if it violates the policy without agent.
- The solution should be able to identify data leaked in the form unknown and known encrypted format like password protected word document.
- The solution should have 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.
- The solution should be able to detect the data leaks over to competitors and the data sent and uploaded after the office hours predefined patterns.
- The solution should provide capabilities to identify data based on keywords or dictionaries and the solution should be able to enforce policies based on file types, size of files and also the name of the file
- The solution should be able to provide risk scores of the user based on their Incident patterns

3.3 Defining exclusive Framework/Policy on Data Governance

Bidder has to define the framework/policy on data governance to ensure data and assets are used properly and managed consistently covering few common areas such as;

- Data quality
- Data Availability
- Data usability
- Data integrity
- Data security

The Data Governance Framework/Policy should also cover the following requirements:

- Defining the role of a nodal officer who is responsible for implementing/overseeing data governance and defining other roles and responsibilities of various stakeholders of DLB with respect to the data governance framework.
- Secure practices to ensure that all types of data and meta-data used in DLB's enterprise are continually identified, managed, protected, inventoried, and classified based on appropriate security classification.
- The various nomenclatures used within DLB to identify and classify data (Example: Customer Data, Payment data, sensitive customer data, critical data etc).
- Define various data classification categories defined by DLB (e.g. public, sensitive, confidential/secret, private etc.) as part of its information security process and identify the types of data that fall under different data classification categories as defined by DLB.
- Cover various types of data such as customer data, sensitive data, Sensitive Personal Data and Information (SPDI), and Personally Identifiable Information (PII).
- Identify the data elements constituting customer data, associated technical data elements (eg. terminal id, geotag, device profile, etc.), Sensitive Personal Data and Information (SPDI), PII and sensitive data.

3.4 Defining Policies and Procedures for Identification, Classification and Protection of Sensitive data

- Bidder will have to develop processes that are required to support the use of the tool/ technology which includes :
  - ✓ Admin Guide, Policy creation, Policy Fine Tuning, Incident management, classification, incident response/ reporting.
- For applying appropriate level of security and also for conducting regulatory/legal assessments, bidder will have to define policies and procedures for identification, classification and protection of sensitive data using encryption. Policies and procedures should be well-defined, aligned with the sensitivity of specific data types.
- Sensitive data should be identified and classified by using nomenclatures such as Public, Internal, Confidential and Restricted.
- As part of security policy, bidder has to define the various data states Data at rest, Data-in-transit) for data protection and also bidder should clearly define the data security measures, tools, technologies used for protecting data-in-transit; in respect of its critical/sensitive/customer data.

3.5 Information Security and Audit

Bidder will have to comply with all the present and future provisions of the Information Security Policy/NPCI Guidelines/Guidelines of RBI, Respective Government Agencies and the Bank and provide such regulatory requirements at no additional cost to bank during the service contract period. The Solution may be audited by RBI/any other Regulatory Authority and any observation pointed out by these bodies have to be complied by the vendor within the timelines stipulated by the regulatory agencies, without any additional cost to the Bank. The

offered solution shall be subjected to Bank's audit through off-site and on-site scrutiny at any time during the contract period. The auditors may be internal/external. The vendor should provide solution and implementation for all the audit points raised by bank's internal/external team during the contract period, within the stipulated timelines, without any extra cost.

3.6 Maintain a Repository of all data classified as sensitive

The proposed DLP solution should have central web-based management console and incident repository. Bank administrators shall use the console to define, deploy and enforce data loss policies, respond to the incidents, analyze and report violations, and perform system administration.

3.7 Data Governance and controls to secure sensitive data

- Bidder is responsible for mapping end-to-end data flows across technology stack so as to identify locations of presence of sensitive/customer data, both within bank premises and externally.
- Security controls should be applied to critical/sensitive data of the bank in hybrid cloud (as part of any application or process managed by bank or third party service provider) to protect data.
- Confidentiality shall be ensured to the encrypted backup tapes where sensitive/ critical data stored.
- Detective security controls shall be put in place to identify unauthorized access to critical sensitive data across technology stack.
- Sensitive data used in non-production environments and processing environments outside the control of the bank shall be protected adequately.

3.8 Resources

All the resources provided for implementation of the solution should be OEM certified or have sufficient levels of experience in implementing the solution at various other clients. It is expected from the partner to share the resource cost for handling DLP incident desk as an optional component.

3.9 Training

Selected bidder shall provide the training to the Bank's personnel as described below:

- ✓ The training should include the architecture, hardware, software, integration, and customization, policy installation, troubleshooting reporting and other aspects of the solution.
- ✓ The Bidder shall train Bank personnel for independent operation, creation of policies/rules, generation of reports, and analysis of the reports, Troubleshooting and familiarization of features and functionalities, policy configuration, alert monitoring, etc. post implementation.
- ✓ Bidder should submit detailed course content and provisional agenda along with the Bid.

- ✓ Refresher training - Post acceptance test, selected bidder shall conduct more refresher trainings for the Bank's team on yearly basis. The participants of these programs may or may not be same.

4. DEPLOYMENT MODELS & SERVICE DELIVERY METHODOLOGY

The Bank is envisaging a model that will be a combination of onsite and remote services offered by the Bidder. Bidder has to perform the following:

- Support centralized deployment, administration, management, and reporting for DLP (email channel).
- Manages all DLP security products (e.g., software, appliances) from one administration console.
- Provides intuitive and easy installation, setup, deployment, population of policies, and ongoing support.
- DLP solution should also provide Monitor appliance which can be installed in sniff mode configuration at the outgoing gateways to monitor outgoing protocol traffic through sniff mode without configuring the traffic in in-line mode configuration as in the case of email gateways.
- DLP solution upgrades should be simple and require very little downtime which ensures that Bank will not miss important events on our network.
- The OEM to provide 24x7 technical support through phone and Web, Product Upgrades, Updates, Patches and access to Technical Library and Product Documentation during any major business outage
- DLP solution modules should include data-in-motion.
- The OEM should take ownership of deployment and directly provide highest premium support offering 24X7 for the solution during the contract period. The implementation can be done by its implementation partners
- The solution should be able to provide alerts whenever there is a policy violation
- The DLP solution should integrate with the 3rd party e-mail gateway to send a violation response to the sender of the e-mail and the e-mail gateway solution should take a quarantine action on the violation. Only the authorized administrator in consultation with Infosec team shall provide permissions for the release of such email.
- The solution should allow creation of custom patterns and the vendor should also create custom patterns based on the banks needs without any additional cost.
- Tool should comply with PCI DSS requirements.
- Enable the classification of email and documents in accordance with PCI information classification requirements.
- Clearly identify information sensitivity by reading classification tags deployed in current environment.

- Enhance the ability of other PCI implementer security solutions to protect sensitive information.

5. SERVICE LEVELS & THRESHOLDS

Service levels provide for minimum level of services required as per contractual obligations based on performance indicators and measurements thereof. The services provided by the bidder shall be reviewed by the Bank on a quarterly basis and Bank shall:

- Check performance of the bidder against defined service levels over the review period of 3 month and consider any key issues of the past period's performance statistics including major incidents, service trends, etc.
- Discuss escalated problems, new issues and matters still outstanding for resolution.
- Review of statistics related to rectification of outstanding faults and agreed changes.
- Obtain suggestions for changes to improve the service levels.

In case, if desired, Bank may initiate an interim review to check the performance and the obligations of the service provider. The Bank will conduct quarterly review of the services rendered by the Service Provider at mutually agreed schedules, dates and representatives from both the Bank and Service Provider should attend such performance review meetings. The Service Levels may be reviewed periodically i.e. quarterly and revised, if required.

The Bank shall have the right to inspect/audit the DLP and Data Classification solution, Tools, Techniques and procedure adopted by the Service Provider in line with security activity outsourced by the Bank, independently or through the outsourced experts and call for detailed report without compromising the Service Provider's Security.

The service levels shall take into consideration the following aspects-

- Equipment Availability Related Service Levels
- Technical Support desk Services
- Compliance and Reporting Procedures
- Quality and Availability of Required Staff

The following measurements and targets shall be used to track and report performance on a regular basis.

5.1 Severity Levels

Severity Definition during Live operations due to Infrastructure/Functional issues of the proposed solution, the SLA's will be applicable post go-live of DLP Solution at DC, DR and other DLB Offices.

Time taken to resolve the reported problem Severity is defined as:

Level	Function/Technologies
Severity 1	1. Such class of errors will include problems, which prevent users from making operational use of solution. 2. Security Incidents 3. No work-around or manual process available 4. Financial impact on DLB 5. Infrastructure related to providing solution to the DLB users comprising of but not limited to the following: a) Proposed Solution Tools / Application Servers b) Proposed Solution Database Servers / Appliance c) Proposed Solution servers/appliances d) Network components, if any proposed by the bidder
Severity 2	1. Any incident which is not classified as "Severity 1" for which an acceptable workaround has been provided by the Bidder or; 2. Any problem due to which the Severity 2 infrastructure of the proposed solution is not available to the DLB users or does not perform according to the defined performance and query processing parameters required as per the RFP or; 3. Users face severe functional restrictions in the application irrespective of the cause. 4. Key business infrastructure, systems and support services comprising of but not limited to the following: a) DLP solution Test & Development and Training Infrastructure and Application b) Infrastructure for providing access of dashboards, scorecards, etc.
Severity 3	1. Any incident which is not classified as "Severity 2" for which an acceptable workaround has been provided by the Bidder; 2. Moderate functional restrictions in the application irrespective of the cause. Has a convenient and readily available workaround.

Level	Function/Technologies
	3. No impact on processing of normal business activities 4. Equipment/system/Applications issues and has no impact on the normal operations/day today working. 5. All other residuary proposed solution Infrastructure not defined in "Severity 1" and "Severity 2"

5.2. Warranty and Support

All the hardware, software products supplied should carry a minimum warranty of 3 - year from the date of operationalization of the system to the satisfaction of the Bank. On-site, comprehensive, back-to-back from Original Equipment Manufacturer (OEM) for a period of 3 years from the date of installation (if applicable). The warranty also includes all software subscriptions (critical hot fixes, service packs, and major upgrades). Remote access to the systems supplied will be permitted through secured VPN connection. Date of start of Warranty/Annual Maintenance/software license support of all the items supplied will be treated as started from the completion of the project.

5.3. Annual Maintenance Contract (AMC)

The AMC shall be:
• On-site, comprehensive, back-to-back from OEM for all hardware and software products as part of RFP for a period of 4 years from the date of expiry of warranty.
• Software updates and upgrades at no cost to Bank.
• L2 and above support from OEM
• Replacement of failed hardware (if applicable) within 24hrs from the time call is lodged.
• Comprehensive on-site support from bidder for day to day operational issues as and when arises.

5.4. Subcontracting

The selected Bidder shall not subcontract or permit anyone other than its personnel or the OEM supplier to perform any of the work, service or other performance required of the vendor under the contract without the prior written consent of Bank.

The successful Bidder will have to participate in periodic meetings with the Bank to discuss project progress and various issues concerning efficient and timely execution. If at any time it should appear to the Bank that the actual progress of work does not conform to the approved milestones, the Bidder shall produce at the request of the Bank a revised timeline showing the modification to the approved timelines necessary to ensure successful operation of the DLP and Data classification solution of the Bank.

In case during execution of services the progress falls behind schedule, then the Bidder should notify the Bank in writing about the same with proper causes for the delay and recovery procedures mentioned. Bidder shall deploy extra manpower, resources to make up the progress. The plan for deployment of extra manpower/ resources will be submitted to the Bank for its review and approval. All time and cost effect in this respect shall be borne by the Bidder.

6. PERIOD OF CONTRACT

The contract will be valid for three (3) years from the date of commencement of the contract subject to yearly review. Bank will enter into a service level agreement with successful bidder for a period of three (3) year from the date commencement of contract.

Date of commencement of contract shall be date of acceptance of the letter of award (Starting Date) or such other date as may be fixed by DLB. The same date shall be considered for renewal of services etc., if applicable.

7. INSTRUCTION TO BIDDERS

7.1 General Instructions

The Bidder is expected to examine all instructions, forms, terms and specifications in the Bidding documents. Failure to furnish all information required by the Bidding/Tender/RFP documents may result in the rejection of its Bid and will be at the Bidder's own risk.

- No binding legal relationship will exist between any of the Bidders and DLB until execution of a contractual agreement, except the pre-contract integrity pact to be submitted along with the Bid. Post evaluation and finalization of the Bids and identification of the successful Bidder, the integrity pact for part of the definitive agreement to be signed by the successful Bidder. For the other Bidders, the pre-contract integrity pact will be binding on them for any acts/omissions committed by the Bidder in violation/breach of the said pre-contract integrity pact in relation to the Bid submitted.
- All costs and expenses incurred by the Bidders in any way associated with the development, preparation, and submission of responses, including but not limited to; the attendance at meetings, discussions, demonstrations etc. and providing any additional information required by DLB, will be borne entirely and exclusively by the Bidder.
- Each Bidder acknowledges and accepts that DLB may in its absolute discretion apply selection criteria specified in the document for evaluation of proposals for short listing / selecting the eligible Consultant (s).
- Every Bidder will, by submitting his Bid in response to this RFP, be deemed to have accepted the terms of this RFP and the Disclaimer.

- Bidders are required to direct all communications related to this RFP, through the nominated Point of Contact persons.
- The Bidder shall bear all the costs associated with the preparation and submission of their bid.
- Bidder should submit the bid strictly as per RFP failing which bid will be rejected as non-responsive.

- Bank may, at its discretion, extend the deadline for submission of bids.

The technical and commercial response evaluation will be based on the criteria described in following section onwards.

7.2 Other Instructions

Bank reserves the right to :

- Not to bind itself to accept the lowest or any Bid and reserves the right to reject any or all bids at any point of time prior to placing the order without assigning any reasons whatsoever**.**
- Waive or Change any formalities, irregularities, or inconsistencies in proposal format delivery.
- Modify the RFP document.
- Apply Bank's own evaluation criteria deemed appropriate for evaluation of both Technical and Commercial Bids.

During Technical evaluation Bank at its discretion can ask the bidders for the detailed presentation of the solution provided.

8. BIDDING PROCESS

A two stage bidding process will be followed. The response to the present tender will be submitted in two parts:

a) Technical bid
b) Commercial bid (Shall need to submit after the technical round if bidder is shortlisted).

Technical Bid shall contain all the supporting documents regarding eligibility criteria, scope of work, Technical aspects, Compliance statement and Terms & Conditions etc. mentioned in the RFP. Only those bidders confirming compliance to all the terms & conditions of RFP document shall be short-listed for commercial stage.

9. MODIFICATION OF BIDS AND CONTACTING THE BANK

9.1 Bids once submitted will be treated as final and no further correspondence will be entertained on this. No bid will be modified after the deadline for submission of bids.

9.2 Any effort by a bidder to influence the Bank in evaluation of the bid, bid comparison or contract award decision may result in the rejection of the bidders bid. Bank decision will be final and without prejudice and will be binding on all parties.

9.3 No Bidder shall contact the Bank on any matter relating to its Bid, once after technical evaluation is over.

10.TERMS & CONDITIONS OF THE BIDDING FIRMS

The bidding firms are not allowed to impose their own terms and conditions to the bid and if submitted will not be considered as forming part of their bids. The bidders are advised to clearly specify the deviations, in case terms and conditions of the contract applicable to this invitation of tender are not acceptable to them.

11.SYSTEM DEMONSTRATION & PROOF OF CONCEPT

Bidder shall conduct Proof of Concept / System Demonstration wherein the Bidder has to demonstrate the implementation of the solution as per the requirement of the DLB. The Bidder shall submit detailed reports of the test outcomes to the DLB. Bidder may highlight the noteworthy/superior features of their solution by reference calls and site visits. The Bidder will demonstrate/substantiate all or a few of the claims made in the Technical Bid to the satisfaction of the DLB, the capability of the solution to support all the required functionalities at their cost in their lab/office/in any other organization where solution is in use. The Bidder should use their own tools/utilities/simulators to demonstrate the features laid in the RFP/evaluation criteria.

12. ELIGIBILITY CRITERIA

Eligibility Criteria for Bidder:

Sl.No.	Eligibility Criteria	Documents to be Submitted
1	The bidder must be an Indian firm/ organization registered under Indian Companies Act.	Copy of Certificate of Incorporation issued by Registrar of Companies
2	The bidder should have a minimum turnover of Rs.2Crores in each year (for last 3 audited Financial Years) in relevant services	Copy of the audited Annual Reports and /or certificate of the Chartered Accountant
3	The bidder should not be currently blacklisted by any Central/State Govt. dept. /Public Sector Unit	Certificate from the Chief Executive / Authorized Officer of Company
4	The bidder should be Original Equipment Manufacturer [OEM] or authorized partner of OEM.	In case of authorized partner of OEM the bidder should submit Manufacturer Authorization Form (MAF) as per format given in **Annexure 4**

5	The proposed DLP Solution must have been successfully provided or currently being provided in at least 2 PSU/ BFSI/ Govt. Organizations in India, during last 3 years as on bid submission date.	Copy of order and/or certificate of completion of the work.
6	The vendor/bidder must have its own support offices in India.	
7	The vendor/bidder must have successfully implemented the DLP solution in at least 2 PSU/ BFSI/ Govt. Organizations in India.	Copy of completion of the work.

Eligibility criteria for OEM:

Sl.No.	**Eligibility Criteria**	**Documents to be Submitted**
1	The DLP Solution should have been successfully completed in at least two banks across globe. Proposed Solution should be from a single OEM covering all channels mentioned as part of the scope	Bidder & OEM Self-Declaration as a part of Covering letter
2	The OEM should not be currently blacklisted by any Central/State Govt. dept. /Public Sector	Non-Blacklisting declaration
3	The OEM must have its must have its own support offices in India	Details support Offices and support system is required

13. BANK'S RIGHT TO ACCEPT OR REJECT ANY BID OR ALL BIDS

The Bank reserves the right to accept or reject any bid and annul the bidding process or even reject all bids at any time prior to award of contract, without thereby incurring any liability to the affected bidder or bidders or without any obligation to inform the affected bier or bidders about the grounds for the Banks action.

14. EVALUATION AND AWARD CRITERIA

14.1 Technical bids will be evaluated based on the eligibility criteria defined in the RFP document. Technical bids of only those bidders satisfying **ALL** the eligibility criteria will be further evaluated.

14.2 Commercial bid's of only those bidders will be considered who qualify technical evaluation.

14.3 A bid submitted with an adjustable price quotation will be treated as non-responsive and rejected.

14.4 Bank purchase committee will evaluate the commercial bid of all technical qualified bidders.

14.5 Bank purchase committee will select successful bidder based upon the Technical evaluation and commercial Bid submitted.

14.6 Bank is not bound to accept the best evaluated bid or any bid and reserves the right to accept any bid, wholly or in part or to reject any or all bids.

15.PENALTY

Penalty would be levied based on the following:

15.1 For service delays, there shall be a penalty of maximum 20% of the total cost of that solution from the finalized Bidder for the Bank.

15.2 Penalties will be levied @ Rs. 1,00,000/- per instance or equal to the loss of amount due to breach will be deducted whichever is higher for violations of rules configured to prevent fraud and/or generate alerts etc. The penalty will be restricted to the 10% of yearly payout value.

16.CONFIDENTIALITY

The bidder shall not, without the written consent of the Bank, disclose the contract or any provision thereof, any specification, or information furnished by or on behalf of the Bank in connection therewith, to any person(s). The bidder shall not, without the prior written consent of the Bank, make use of any document or information except for purposes of performing this agreement

17.DUE DILIGENCE

Bidder shall allow DLB or its authorized representatives to conduct, due diligence of the out sourced vendors on a yearly basis. DLB or its authorized representatives shall have the right to inspect and audit the books, records and information of the Service Provider at any point of time after giving a prior written intimation of 7 days and shall also state the day and time of such inspection and specifying the Bank officials who shall undertake such inspection for the services under this Agreement.

RBI or persons authorized by it shall be allowed to access/inspect the Bank's documents, records of transactions, and other necessary information given to, stored or processed by the service provider within a reasonable time.

18.FRAUD PREVENTION

Fraud, if any, committed / attempted by the service provider or its resources as part of this engagement shall be brought to the notice of Bank's vigilance department at central office then and there and the same will be dealt with as per the Bank's policy on fraud prevention control.

19.PATENT RIGHTS

19.1 The supplier shall indemnify the purchaser against all third party claims of infringement of patent, trademark or industrial design rights arising from use of the Goods, or any part thereof in India.

19.2 The supplier shall, at their own expense, defend and indemnify the Bank against all third party claims or infringement of intellectual Property Right, including Patent, trademark, copyright, trade secret or industrial design rights arising from use of the products or any part thereof in India or abroad.

19.3 The supplier shall expeditiously extinguish any such claims and shall have full rights to defend itself there from. If the Bank is required to pay compensation to a third party resulting from such infringement, the supplier shall be fully responsible therefore, including all expenses and court and legal fees.

20.SIGNING OF CONTRACT

The successful bidder(s) shall mandatorily enter into a Service Level Agreement (SLA), and Non-Disclosure Agreement (NDA) with Bank, within 30 days of the award of the tender or within such extended period as may be permitted by the bank. The letter of acceptance and such other terms and conditions as may be determined by the Bank to be necessary for the due performance of the work in accordance with the Bid and the acceptance thereof, with terms and conditions shall be contained in a Memorandum of Understanding to be signed at the time of execution of the Form of Contract.

21.PAYMENT TERMS

Dhanlaxmi Bank Ltd will make payment as follows:

Payment Milestone:

- 30% along with PO
- 30% after solution is deployed
- 40% after completion of 6 months of service

There shall be no escalation in the prices once the prices are fixed and agreed to by the Bank and the vendor. Payment will be released by ISG Dept, as per above payment terms on submission of Original GST invoices to bank.

Bid shall be submitted in Hard/Soft Copies. The bid should contain following:

1. Technical Bid.
2. Commercial Bid. Price shall be submitted as per format **Annexure -3**

Address for Communication:

Ms.Seetha Vimal
Assistant Manager – Information Security Group
Dhanlaxmi Bank Limited
3rd Floor, Corporate Office,
Dhanalakshmi Buildings
Punkunnam, Thrissur,
Kerala – 680 002
Phone: 0487 7107336
Email: seetha.vimal@dhanbank.co.in

22.CLARIFICATIONS REGARDING RFP DOCUMENT

Before bidding, the bidders are requested to carefully examine the RFP Document and the terms and conditions specified therein. In case the bidders require any clarification on this RFP, the query may be sent to e-mail addresses: ranjith.p@dhanbank.co.in and seetha.vimal@dhanbank.co.in.

23.IMPORTANT DATES

Sl no	Particulars	Date
1	Issuance of RFP document by the Bank	6th May 2022
2	Last date of submission of any queries, clarifications etc.	13th May 2022
3	Last Date of submission of RFP response as soft copy	20th May 2022

24.EXECUTION OF AGREEMENT

On awarding the contract, the successful bidder and Bank should execute an agreement, which states the responsibilities and obligations of each party with the other, as per bank's outsourcing policy. The Bidder should sign and execute this Non-Disclosure Agreement before the execution of this Contract. The contract will be for a period of five year.

The Technical Bid / Scope of the Work submitted by the Bidder will be evaluated based on the terms and conditions of the RFP. Detailed technical evaluation will include, scrutiny of company profile, technical and functional information of proposed software/service solution, system demonstration of proposed solution, reference calls and site visits.

The functional and technical specification is in a form of a table as provided in **Annexure-1**, which contains the required functionality features in the second column. Bidder's responses against each functionality as detailed therein would be evaluated for the selection.

1. To meet DLB's requirements, as spelt out in this Bid Document, the selected Bidder must have the requisite experience and expertise in providing services in the field of

information and communication technology, the technical know-how, and the financial ability that would be required to successfully set-up the required infrastructure and provide the services sought by DLB.

2. A screening committee constituted by DLB for the purpose of selection of the successful Bidder, would evaluate Bids.

3. The proposals will be evaluated in stages. In the first stage, i.e. Technical Evaluation of the Bidders will be done and in the second stage. Indicative commercial bids would be evaluated and commercial negotiation/Price discovery will be conducted for the technically qualified bidders in this stage.

4. The Technical Bid should necessarily contain all Technical details and other terms and condition of RFP. Bidder's proposal should conform to the contents and format of the technical bid listed out **Annexure-1** of the RFP. Proposals not conforming to the specifications may be rejected summarily. Any incomplete or ambiguous terms/conditions will disqualify the offer.

5. The Technical Bid submitted by the Bidder will be evaluated based on the terms and conditions of the RFP. Detailed technical evaluation will include scrutiny of company profile, technical and functional information of proposed software/service solution, and system demonstration of proposed solution, reference calls and site visits.

6. Each Bidder acknowledges and accepts that DLB may, in its absolute discretion, apply whatever criteria it deems appropriate in the selection of vendor, not limited to those selection criteria set out in this RFP document.

7. The Bidders shall be short listed after the evaluation of their Technical Bids and will be informed. Only the short listed bidders will be permitted to participate further process.

8. DLB reserves the right to modify / amend the evaluation process at any time during the Bid process, without assigning any reason, whatsoever, and without any requirement of intimating the Bidders of any such change. At any time during the process of Bid evaluation, DLB may seek specific clarifications from any or all Bidders.

9. DLB reserves the right to modify the total quantities subject to a variation of ± 25% on either side of the projected requirements during the rate contract i.e. three years (3) from the date of award of the contract. The Bidder shall not and hereby waive any or all objections that it might have at the relevant point of time.

10. Bidder will not be invited for opening of Indicative commercial bid after qualifying in the Technical Bids.

11. DLB reserves the right to accept or reject in part or full any or all the Bids without assigning any reason whatsoever. Any decision of DLB in this regard shall be final, conclusive and binding on the Bidder.

12. DLB reserves the right to re-issue / re-commence the entire bid process in case of any anomaly, irregularity or discrepancy in regard thereof. Any decision of the DLB in this regard shall be final, conclusive and binding on the Bidder.

13. Modification to the RFP Document, amendments, time-extension, clarification etc. if any, will be made available as an addendum on the DLB's website and / or emailed to the prospective Bidders.

14. The Bidder should confirm in writing its obligation to supply upgraded model of the product in case of technological obsolescence / non-availability of contracted product/model. The supply of upgraded product, subject to the DLB's approval, will be at the same contracted price as the obsolete model.

15. In case of reduction of prices due to technological obsolescence / change of product model, the Bidder should pass on the price benefit to the DLB.

16. Successful Bidder would sign the Contract/SLA and other forms specified in RFP Document with Dhanlaxmi Bank at Thrissur only.

17. The Bidder shall bear all costs and expenses for the execution, stamp duty and submission of the contract and agreements. DLB shall not be responsible or liable for reimbursing/compensating these costs and expenses.

18. To complete the work at the site within stipulated timeframe, Bidder's employees/workmen may have to visit the site multiple times, at no extra cost to the DLB.

19. Quotations contained in the Bids shall remain valid for a period of 90 (ninety) days from the date of submission of the Bid in response to the RFP.

20. Prices quoted should be EXCLUSIVE of all applicable taxes and TDS would be deducted at source, if any, as per prevailing rates.

21. The price ("Bid Price") quoted by the Bidder cannot be altered or changed due to escalation on account of any variation due currency exchange rates or cost of material.

22. The DLB will not be obliged to meet and have discussions with any Bidder and/ or to entertain any representations in this regard.

23. During the period of evaluation, Bidders may be asked to provide more details and explanations about information they have provided in the proposals. Bidders should respond to such requests within the time frame indicated in the letter/e-mail seeking the explanation.

24. The Bids received and accepted will be evaluated by the DLB to ascertain the best and lowest bid in the interest of the DLB. However, the DLB does not bind itself to accept any Bid, lowest or otherwise, and reserves the right to reject any or all bids at any point of time prior to the order without assigning any reasons whatsoever.

25. Apart from the above, the company profile, past experience and performance track record of the Bidder in the area of the assignment, methodology to be adopted to carry out the assignment, delivery schedule, service support, price, etc. shall be some of the important criteria in selecting the bidder.

26. The Bids will be evaluated both on the Technical and Commercial merits and the DLB's decision in this regard shall be binding, final and conclusive.

25.TERMINATION OF CONTRACT

The quality of services given by the bidder & progress of the project will be reviewed monthly and if the services are not found satisfactory, the Bank reserves the right to terminate the contract by giving 30 days' notice to the bidder, including 15 days curing period. The decision of the Bank regarding quality of services shall be final and binding on the bidder.

The Bank shall have the right to terminate/cancel the contract with the selected bidder at any time during the contract period, by giving a written notice of 30 days, for any valid reason, including but not limited to the following:

a) Excessive delay in execution of order placed by the Bank
b) Discrepancies / deviations in the agreed processes and/or products
c) Failure of vendor (successful bidder) to complete implementation of appliance within the time as specified in the RFP document
d) Violation of terms & conditions stipulated in this RFP.
e) Exceeding any of the threshold limit of Delay
f) Non fulfillment of SLA agreement

Notwithstanding anything contained hereinabove, the Bank reserves the right to terminate the contact at any time without assigning any reasons. In case of termination of contract for the reasons that the services of vendor are not found satisfactory", the Bank shall be free to Blacklist the vendor thereby debarring them from participating in future Bids/Tender processes

26.ANNEXURES

Bidders meeting the eligibility criteria have to submit their Bids along with supporting documents and with all filled annexure. If the Bid is not accompanied by all the required documents supporting eligibility criteria, the same would be rejected

List of Annexures

Annexure-1 Technical Specification of DLP
Annexure-2 Technical Specification of Data Classification Solution
Annexure-3 Commercial Bid Format
Annexure 4 OEM/Manufacturer Authorization Format
Annexure-5 Non Blacklisting Declaration Format (On OEM's letter head)
Annexure-6 Eligibility Criteria
Annexure-7 Acceptance of Terms & Conditions

Annexure -1

Technical Specification of DLP

Sl no.	Specifications	Complied (Yes/No)	Remarks
	Email DLP		
1	The solution should provide the central management for the incidents generated over the Email, and discovery		
2	The solution should be able to block outbound emails sent via SMTP if it violates the policy without agent.		
3	The proposed solution should work as an 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, this should be achieved on solution same solution itself		
4	The solution should be able to identify data leaked in the form unknown and known encrypted format like password protected word document. The solution should be able to identify malicious traffic pattern generated by Malware infected PC in order to prevent future data loss by the malware. The solution should support quarantine as an action for email policy violations and should allow the sender's manager to review the mail and provide permissions for him to release the mail without logging into the UI		

Sl no.	Specifications	Complied (Yes/No)	Remarks
	Automated Response & Incident Management		
5	The 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 possible.		
6	The solution should support quarantine as an action for email policy violations and should allow the sender's manager to review the mail and provide permissions for him to release the mail without logging into the UI		
7	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		
8	The incident should display the complete identity of the sender (Full name, Business unit, manager name etc.) and destination of transmission for all network and endpoint channels. The solution should also allow assigning of incidents to a specific incident manager		
9	The solution should provide automatic notification to incident managers when a new incident is assigned to them, and the incident		

Sl no.	Specifications	Complied (Yes/No)	Remarks
	should not allow for deletion even by the product administrator		
10	The solution should allow a specific incident manager to manage incidents of specific policy violation, specific user groups etc.		
	Role Based Access and Privacy Control		
11	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		
12	The system should create separate roles for technical administration of servers, user administration, policy creation and editing, incident remediation, and incident viewing for data in motion.		
13	The system should allow a role only to view incidents but not manage or remediate them		
14	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.		
15	The system should allow incident managers and administrators to use their Active directory credentials to login into the console		

Sl no.	Specifications	Complied (Yes/No)	Remarks
	Reporting and Analytics		
16	The solution should have a dashboard view designed for use by executives that can combine information from data-in-motion (email).		
17	The system should allow reports to be mailed directly from the UI and should allow automatic schedule of reports to identified recipients		
18	The reports should be exported to at least CSV, PDF formats		
19	The proposed solution should provide Incident Workflow capabilities where user/Business Manager can remediate the email DLP policy violations actions from handsets/emails without logging into the Management Console		
20	The email 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.		
21	The DLP dashboard must display the number of cases in the designated period that fall above the risk score threshold that you have selected. Risk score thresholds must be customizable and instantly produce a report to prioritize the cases from high-to-low risk levels by leveraging analytics or machine learning technologies.		
22	Solution should support components on TLS 1.2		

Annexure -2

Technical Specification of Data Classification Solution

SI no.	Specifications	Complied	Remarks
1	The solution should evaluate content, context, identity, and other attributes of unstructured data to make classification, categorization, and policy decisions.		
2	The solution should support automated, suggested, and user-driven classification.		
3	The solution should label email documents.		
4	The solution should label documents with visual markings such as watermarks, header, or footers. The files will need to be electronically marked.		
5	The solution must be able to integrate with Microsoft cloud services and applications, such as Office 365 and Azure Active Directory. It must be used with line-of-business applications and information protection solutions from software vendors, whether these applications and solutions are on-premises, or in the cloud.		
6	The solution must have monitoring and detection capabilities. Once a document has been classified and marked the solution must have the flexibility to set up actions to be taken including blocking transmission of the document, and provide a warning to the sender, send		

SI no.	Specifications	Complied	Remarks
	notification to the creator or owner of the document, or send notification to the administrator.		
7	The solution should be able to monitor for policy warnings and violations and have the flexibility to report via text, email, or console view.		
8	The solution must have the capability to provide on demand, daily, weekly and trending reports showing all policy violations and warnings including trending over a prescribed period. The reports should show an analysis of documents that have been automatically classified as well as a historical view of all documents.		
9	The solution should have auditing capabilities to ensure that documents are continuing to be classified in an accurate and consistent basis.		
10	The bidder will be responsible for the implementation and support of the solution including training to the employees. The bidder should provide a detailed project plan of the activities required in the implementation process, including all tasks, milestones, and timeframes, by providing a chart or graphic.		
11	The solution should support policy conditionality based on data attributes like content, classification, recipients, sender, author, filename, path, IP address, MAC address, modification date, file type, and location.		

SI no.	Specifications	Complied	Remarks
12	The solution should interact and educate users about proper data handling at the exact time they are creating, handling, sharing or saving files.		
13	The solution should support policy conditionality based on data attributes like content, classification, recipients, sender, author, filename, path, IP address, MAC address, modification date, file type, and location.		
	INFORMATION PROTECTION		
14	The solution should support functionality to check recipients marked in an email and alert/prevent the user from sending the mail if external recipients are marked. Example : An email containing internally classified document as attachment should be prevented from being sent if external recipients are marked in that mail. The user should also get an alert for the same.		
15	Provides fine-grained control over the policy actions that apply to different use cases, such as when to classify automatically, via machine learning, and/or when to prompt the user.		
16	The solution should support creation of policy which can embed specific actionable information (eg: Sensitivity, data retention/legal holds, regulation applicability, information type, diagnostic codes, etc).		
17	The solution should be able to identify information like Aadhar,		

SI no.	Specifications	Complied	Remarks
	Passport numbers, credit card information for automated classification thru either inbuilt capability or should have capability to define regular expressions.		
18	The solution should have capability to detect differential classification between an email and its attachments and block the email from being sent.		
19	The solution should support different classification values for different applications. This can be combined with user targeting to present detailed classification options based on application and user identity. For example, users in the accounting department may be able to capture additional accounting and retention metadata for Excel files, but use a simplified classification schema for email.		
20	The solution should support the ability to natively allow password to protect/encrypt sensitive files by throwing a pop-up whenever user is trying to share confidential file to authorized recipients.		
21	The solution should provide the ability to warn/prevent users from downgrading or changing a classification		
22	The solution should provide the ability to allow only specific users and AD groups to downgrade, upgrade and change classification		

SI no.	Specifications	Complied	Remarks
23	The solution should provide the ability to warn users when opening sensitive Office documents natively.		
24	The solution should provide the ability to prevent printing of sensitive email and Office documents based on classification to specific printers natively.		
25	The solution should provide the ability to highlight sensitive information within an MS outlook email and redact the sensitive content so that users can remediate any policy violations before the email leaves the desktop.		
26	The solution should provide advanced control over email via policies that evaluate content, recipients, sender, classification, filename, file size, and other attributes		
27	The solution should support the ability to restrict email based on sender. For example, one user may be authorized to send sensitive information externally, but others are not allowed to do this. The policy decision may be based on the sender's email, name, or AD attributes or group membership.		
28	The solution should support policy combinations to enable more advanced use cases, such as checking whether a document is having regulatory data, and then blocking an unauthorized user from sending the		

SI no.	Specifications	Complied	Remarks
	document as an attachment in mail.		
29	The solution should support multiple classification types (i.e. dropdowns, multi-selects, date fields, and user typein).		
30	The solution should provide the ability to evaluate the number of instances of sensitive data within a document, and then apply the appropriate policy. For example, users may be allowed to save a document with one credit card number as General Business, but if there is more than one unique credit card number, the document should be saved automatically as restricted classification.		
31	The solution should provide the native ability to restrict users from sending non-classified email attachments for MS Outlook (i.e. attachments that have no classification).		
32	The solution should be able to label the documents in Headers/Footers with a preselection capability for either header or footer or both.		
33	The solution should be able to track initial classification and reclassification events at both document and central logging level.		
	AUDITING AND REPORTING		
34	The solution should log user activity while users are handling email,		

SI no.	Specifications	Complied	Remarks
	documents, and files.		
35	The solution should provide flexibility to send user logs to SIEM, syslog server, text file, and Windows event logs as per the need.		
36	The solution should provide a built-in dashboard for reviewing data discovery scanning results for user activity, deployment, data storage trends, and data inventory.		
37	The solution should provide built-in reports and dashboards to analyse user behaviour and system health.		
38	The solution should provide a pre-built starter set of reports for the reporting database (in tab separated values/ Excel or Database format) and Views and documentation to enable customers to write their own reports.		
39	The solution should integrate with third-party reporting tools to provide meaningful reports on user activity and deployment.		
	INTEGRATION AND INTEROPERABILITY		
40	The solution should provide the ability to attach metadata to information objects, which can be leveraged by e-discovery solutions.		
41	The solution should provide the ability to attach metadata to information objects, which can be leveraged by third-party data loss		

SI no.	Specifications	Complied	Remarks
	prevention (DLP) solutions.		
42	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.		
43	The solutions should be able to insert metadata tags in the documents and emails which can be read by DLP, CASB, Backup, Archival and IRM Solutions.		
44	The solution should support the ability to add a user's Active Directory username and group to visual markings when opening sensitive documents. This information provides increased user accountability and can be removed automatically when the user closes the document.		

Annexure-3

COMMERCIAL BID FORMAT

RFP for providing Data Leakage Prevention & Data Classification Solution

Sl no.	Description of Services	Amount
1	**Short Description of the solution & services offered**	

NOTES

1. The rates quoted in commercial bid should be inclusive of all taxes except GST. However, GST shall be paid to the bidder on actual basis at the rate applicable. The rate of applicable
2. GST should be informed and charged separately in the invoice generated for supply of the product.

2. Any column left blank by the bidder will result in disqualification of the bid.

3. L1 cost will be decided as per total of Table A

4. Bidder should quote rates per quarter which will be valid for the period of 3 years from the date of signing of contract.

5. Bank will not be making any other payment except those mentioned in the commercial bid.

Date: _____

Place: _____

Signature of Authorized Signatory

Annexure -4

OEM/Manufacturer Authorization Format *(On OEM's letter head)*
Ref: Date:

To

Chief Information Security Officer
Information Security Group, 3rd Floor
Dhanlaxmi Bank
Corporate Office
Thrissur - 680002

Dear Sir,
Sub: Manufacturer Authorization for RFP No. DLB_ISG/ RFP/ 2022-23/ 001

We <OEM Name>having our registered office at <*OEM Address*>are an established and reputed company/producer/manufacturer of <*product details*>do hereby authorize M/s_____ (Name and address of the Partner) to offer their quotation, negotiate and conclude the contract with you against the above invitation for tender offer.

We hereby extend our full guarantee/warranty/support as per terms and conditions of the tender and the contract for the solution, products/equipment and services offered against this invitation for tender offer by the above firm and will extend technical support and updates / upgrades if contracted by the bidder.

We also confirm that we will ensure all product upgrades (including management software upgrades and new product feature releases.) are provided by *M/s* ……..for all the products quoted for and supplied to Dhanlaxmi Bank during the Three year product warranty/Support period.

<OEM Name>
<Authorized Signatory>

Name:
Designation:

Note: This letter of authority should be on the letterhead of the OEM and should be signed by a person competent and having the power of attorney to bind the manufacturer. It should be included by the bidder in its bid.

Annexure - 5

Non Blacklisting Declaration Format *(On OEM's letter head)*

Ref: Date:

To

Chief Information Security Officer
Information Security Group, 3rd Floor
Dhanlaxmi Bank
Corporate Office
Thrissur - 680002

Dear Sir,

Sub: Non Blacklisting Declaration by <*OEM Name*> for RFP No. **DLB_ISG/ RFP/ 2022-23/001**

We <OEM Name>having our registered office at <*OEM Address*>are an established and reputed manufacturer of <*Name of Product*>, do hereby declare and confirm that we are not currently blacklisted by any Central/State Govt. or any Dept/Bank.

<*OEM Name*>

<*Authorized Signatory*>

Name:

Designation:

Note: This letter of authority should be on the letterhead of the OEM and should be signed by a person competent and having the power of attorney to bind the manufacturer. It should be included by the bidder in its bid.

Annexure - 6

Eligibility Criteria for Bidders for Data Leakage Prevention & Data Classification Solution

Sl.	Pre-Qualification Criteria	Documents need to be submitted	Compliance (Yes/No)
1	The bidder participating in the bid should be registered in INDIA as per the companies act or have its registered office within the jurisdiction of INDIA in last 3 years	Certification of Incorporation	
2	Bidder must be an ISO 27001: 2008 or higher certified company.	Copies of valid certificates	
3	The proposed Solution must have been successfully provided or currently being provided in at least 2 PSU/ BFSI/ Govt. Organizations in India, during last 3 years as on bid submission date. The period for which the services have been availed or are being availed by the client organization should be at least one year	Satisfactory Performance Certificate from the Clients. OR Purchase Order along with Email confirmation from the clients containing all the required information. Kindly note that that Client's Email should be from their official Email IDs only, containing their name, designation & Mobile no. OR Copy of Work Order along with any other proof of successful execution. (Kindly note that any of the above documents submitted must be sufficient enough to certify OEM's/bidder's experience, must be authentic and must also contain all the material information)	
4	The bidder must have successfully provided or currently being provided in at least 2 PSU/ BFSI/ Govt. Organizations in India, during last 3 years as on bid submission date. Out of these two, one experience should be of the OEM whose services are being proposed to Bank through this RFP. The period for which the services have been availed or are being availed by the client organization should be atleast one year		
5	The Bidder should be profitable organization (on the basis of Operating Profit) for at least 3 out of last 5 financial years.	Copy of the audited balance sheets along with profit and loss statement for corresponding years and / or Certificate of the Chartered Accountant	

Sl.	Pre-Qualification Criteria	Documents need to be submitted	Compliance (Yes/No)
6	The bidder should have a minimum turnover of INR 2 Crores (Rs. One Crores) per annum from Information security services, for the past 3 financial years i.e. 2018-19 2019-20 & 2020-21.The bidder should have positive net worth during the last three financial years.	Copy of the audited balance sheets along with profit and loss statement for corresponding years and / or Certificate of the Chartered Accountant	
7	The Proposed OEM should have a presence in India for the last 3 years.	Declaration from OEM.	
8	The Bidder should have support office in at least 4 (Four) Metro Locations (Kolkata, Mumbai, New Delhi, Chennai] and in Bangalore, Hyderabad, Pune.	Self-declaration with office location addresses.	
9	The Proposed Solution (OEM) should not have been blacklisted by Government, any govt. department, PSU or PSB during the last three years.	Self-declaration. (Template available in **Annexure- 3**)	
10	The Bidder should not outsource any of the project activities and it has to be executed by own experienced professionals	Self-declaration from Bidder.	
11	Bidder should have more than 50 security professionals in various cortication's	Self-declaration from Bidder	
12	The Bidders should have Toll Free number for fault registration within India, operating 365x24x7 basis	Self-declaration from Bidder with Toll free number details	

Annexure - 7

Acceptance of Terms and Conditions.

(Letter to the bank on the bidder's letterhead)

To

Chief Information Security Officer
Information Security Group, 3rd Floor
Dhanlaxmi Bank
Corporate Office
Thrissur - 680002

Dear Sir,

Sub: **RFP No: ISG/ RFP/ 2022-23/ 001**

With reference to the above RFP, having examined and understood the instructions, terms, conditions, annexure and amendments forming part of the RFP, we hereby enclose our offer for the supply of the items/equipment/solutions as detailed in your above referred RFP.

We further confirm that the offer is in conformity with the terms/conditions as mentioned in the RFP and all required information /annexure is enclosed. Also we conform that the all information/details enclosed are true and fully aware that if anything is found false/wrong in later stage, it will invite penalties/legal action by Dhanlaxmi Bank.

We also confirm that the offer shall remain valid for two months from the date of the offer.

We also agree that you are not bound to accept the lowest or any bid received and you may reject all or any bid without assigning any reason or giving any explanation whatsoever.

Authorized Signatory Name Designation Office Seal

Place:

Date: