Amendments & Clarifications - Ref: CO:ITD:25/R1:2019-20 dated 10.04.2019 for "Procurement of DLP (Data Leak Prevention) Solution with required hardware / software at Data Centre (Chennai) and DR Site (Hyderabad) with 1 year warranty and 4 years support"

Amendments:

S.no.	References	Existing Clause	Amended Clause
1	Page no. 20 Point no. 18 **SETTLEMENT OF DISPUTES**	Any dispute or difference in respect of which a notice of intention to commence arbitration has been given in accordance with this clause shall be finally settled by arbitration subject to Settlement of Disputes, Para-XII, Clause-5 hereinafter mentioned. Arbitration may be commenced prior to or after delivery of the goods under the contract.	Any dispute or difference in respect of which a notice of intention to commence arbitration has been given in accordance with this clause shall be finally settled by arbitration. Arbitration may be commenced prior to or after delivery of the goods under the contract.
2	Page no. 21 Point no. 23 **LIMITATION OF LIABILITY**	The Purchaser acknowledges that no promise, representation, warranty or undertaking has been or will be made or given by the Successful bidder or any person on behalf of the Successful bidder in relation to the Support Services, the Systems or this Agreement including the quality of the support Services or any goods supplied. The Purchaser has relied upon its own skill and judgment in opting for these services. Save where herein expressly provided, all whatsoever other warranties implied by law are hereby excluded.	Supplier's aggregate liability under the contract shall be limited to a maximum of the contract value. This limit shall not apply to third party claims for a) IP Infringement indemnity. b) Bodily injury (including Death) and damage to real property and tangible property caused by Supplier's gross negligence. For the purpose for the section, contract value at any given point of time, means the aggregate value of the purchase order placed by bank on the Supplier that gave rise to claim, under this tender. c) Supplier shall not be liable for any indirect, consequential, incidental or special damages under the agreement/ purchase order. For (a) and (b) above, the liability is limited to the Compensation awarded by court of law.The liability is capped to Contract value.

3	Page no 31 Clause 2 **QUALIFICATION CRITERIA**	The Bidder should be a profit making company during the last 3 consecutive financial years of the bidder (2015-16, 2016-17 and 2017-18),with a minimum annual turnover of Rs.60.00 Crores during each year out of which at least Rs.20.00 Crores should be from the information security domain.	The Bidder should be a profit making company in 3 out of last 4 financial years of the bidder (2015-16, 2016-17, 2017-18 and 2018-19),with a minimum annual turnover of Rs.60.00 Crores during each year out of which at least Rs.20.00 Crores should be from the information security domain.
4	Page No.31 Clause 4 **QUALIFICATION CRITERIA**	The bidder should have support Centres in Chennai, Hyderabad, Mumbai, New Delhi & Kolkata.	The bidder should have support Centres in Chennai, Hyderabad and should provide support from Mumbai, New Delhi & Kolkata through their own office or through partners.
5	Page no. 40 **PERFORMANCE SECURITY FORM**	Please note that guarantee to be valid for 39 months and claim period is 1 month as per Clause 4(Performance Security) of condition of contract.	Please note that guarantee to be valid for Sixty Six (66) months with further One month claim period as per Clause 3 (Performance Security) of condition of contract.
6	Page No.30 Section IV. (D) Additional specifications for Data Classification tool.	Nil	Please refer to the Annexure.

Clarifications:

S.no.	References	Queries/ Request	Clarification from Bank
1	Page no. 17 Clause no. 9	How the bidder can provide quarterly Availability and performance reports and accountable to manage the same?	It is clarified that the solution should facilitate bank to get the reports from the dashboard.
2	Page no. 18 Clause no. 9	If the bidder is to onetime configure and implement the solution in 4 months and bank's incumbent will do management on-going basis then how the bidder can take responsibility of any breaches and penalties?	It is clarified that penalty will be calculated on the failure of DLP policy configured by the successful bidder or inbuilt in the solution.
3	Page no. 18 Clause no. 9	If there is no on-going support post implementation with bidder, Honouring and adherence of any SLAs related to service or the platform is not achievable. Please elaborate how the bank would like to address it.	SLA will be calculated on response and resolution time from the time of logging the call for the downtime of the solution. Bidder

			has to make solution up within the stipulated resolution time.
4	Page no. 22 Clause no. 26	In the interest of the Bank, we would request you to consider sub-contracting for post implementation support considering the length and breadth of the country as it will be difficult to reach remote areas from presence in the 4 metros also.	It is clarified that engineers who need to visit branches may be from the partners of the successful bidder.
5	Page no. 26 Clause no. 46	Data Classification required dedicated tool - If yes then Bank should give detailed specification (Or) OEM can use the Data Classification templates inside the DLP?	It is clarified that Data Classification is required. For detailed additional specifications on data classification please refer to amendment.
6		Management of the Infra hosted out of customer location- Bank need to allow the management of the Infra from Remote SOC so that Bidder can do the management the Server, OS, compute through our GSMC NMS and share reports.	It is clarified that remote SOC will not be allowed. Bidder has to send an engineer to the Banks's Data Centre/DR Site/Head office/Corporate office whenever required for the said purpose.
7		We need detailed scope of the bidder post implementation including RACI among incumbent and bidder.	Additional Scope of the bidder post implementation is : - To maintain uptime of the solution. - To provide on-call support. To update / upgrade the solution during the contract period. - To ensure that the solution is patched regularly and is free from Cyber threats. - To fix all audit findings of bank team and its auditors. - To support Bank during DR Drill - Should ensure that the logs are reaching SIEM solution.

Annexure

In addition to the existing specification for DLP solution, the data classification tool provided should adhere to the following specifications.

S. No.	Technical Specification	Complied (Yes/No)
1	The solution should evaluate content, context, identity and other attributes of unstructured data to make classification and policy decisions.	
2	The solution should support policy conditionality based on data attributes like content, classification, recipients, sender, author, filename, path, IP address, modification date, file type, and location.	
3	The solution should support automated, suggested, and user-driven classification, Capabilities to do automatic classification.	
4	The solution should enable the classification of Word, Excel, PowerPoint documents.	
5	The solution should support hierarchical and conditional classification fields, so that the appearance of a sub-field is conditional on the value selected in the higher-level field. For example, when a user selects "Restricted," a sub-field is presented with a list of departments including "HR Only."	
6	The solution should enable users to assign classification values to any file type by right-clicking in File Explorer and selecting one or more files.	
7	The solution should support automatic classification of files when its downloaded and saved to specific folders (e.g. Downloads, My Documents) and the classification should be based on file content for files that can be read by a text processor and based on file type or file size or file name or file path for other file types.	
8	The solution should provide the ability to prevent and warn users from downgrading, upgrading, or changing a classification and administrators should be able to configure which users can override policy warnings	
9	The solution should provide the ability to highlight sensitive information within an email and redact the sensitive content so that users can remediate any policy violations before the email leaves the endpoint.	
10	The solution should allow only the file owner mentioned in the file attribute or specific AD groups to downgrade file classification.	
11	The solution should be capable of integrating with SIEM.	
12	The solution should provide the ability to attach metadata to documents and emails, which can be leveraged by third-party data loss prevention (DLP) solutions.	
13	The solution should support customizable policies.	
14	The solution should trigger policy and classification actions based on different events, such as Open, Save, Print, Forward, Close, Send New Email or Classification Change.	
15	The solution should support the ability to prompt users to change the default classification(s) if the default is inappropriate for the content, context, or other attributes of the email or document.	
16	The solution should support the ability to prompt users to classify in some cases, and use automated classification in others. For example, a default classification may be used for internal email, but users are prompted to classify for external email. Or users may be prompted to classify email only when there is an attachment.	
17	The solution should provide the ability to automatically apply classification (and protection) as files are created, moved to, and modified in local directories and mapped drives.	
18	The solution should log user activity while users are handling documents and files.	
19	The solution should provide audit trails for the changes done in policies.	
20	The solution should support all Windows OS (Win7, Win8, Win10 etc.) 32bit and 64 bit.	