Islami Bank
Bangladesh PLC. | Based on Shari'ah

Amendments in the Tender Schedule relating to the Procurement of Data Loss Prevention (DLP) Solution of the Bank are as follows:

Technical Terms and Conditions

B.Compliance of Specifications of Data Loss Prevention (DLP) Solution.

Ext. Sl	Page No/ Annexure	Existing Technical terms & conditions as per Tender Schedule	Amendments
5	Page no 12/ Aneex-II	Data Masking: Dynamic data masking to protect sensitive data by replacing it with fictitious but realistic values.	The solution should Support PrtSc blocking on endpoint when configurable list of specific application are running, no matter it is in the foreground or background. The actual PrtSc capture will also be submitted to the DLP system as forensic evidence.
12	Page no 12/ Aneex-II	Data Encryption: Encryption of sensitive data at rest and in transit, with strong encryption algorithms and centralized key management. **Priority : (M-Mandatory)**	Data Encryption: Encryption of sensitive data at rest and in transit, with strong encryption algorithms and centralized key management. The encryption solution can be built in or 3rd party solution needs to be factored to meet the requirement. **Priority : (D-Desired)**
19	Page no 12/ Aneex-II	Mobile Device Management: Integration with mobile device management solutions to enforce data protection policies on mobile devices. **Priority : (M-Mandatory)**	Mobile Device Management: Integration with mobile device management solutions to enforce data protection policies on mobile devices. **Priority : (D-Desired)**
24	Page no 12/ Aneex-II	Mobile Application Security: Analysis and monitoring of mobile applications to identify security vulnerabilities and data leakage risks. **Priority : (M-Mandatory)**	Mobile Application Security: Analysis and monitoring of mobile applications to identify security vulnerabilities and data leakage risks. **Priority : (D-Desired)**
26	Page no 13/ Aneex-II	Data Masking: Dynamic data masking to protect sensitive data in non-production environments, such as test and development environments.	The endpoint solution should Blocking of non-Windows CD/DVD burners, it should also Inspect and optionally block Explorer writes to WPD class devices. The endpoint solution should encrypt information copied to removable media. It Should support both Native and Portable Encryption and manage the Encryption and DLP policies from the same management Console.

32	Page no 13/ Aneex-II	Data Masking for Reporting: On-the-fly data masking for reports and business intelligence outputs to ensure data privacy.	The system should display the original file location and policy match details for files found to violate policy.
36	Page no 13/ Aneex-II	File Encryption and Rights Management: Encryption of files and implementation of digital rights management (DRM) to control access, usage, and permissions. **Priority : (M-Mandatory)**	File Encryption and Rights Management: Encryption of files and implementation of digital rights management (DRM) to control access, usage, and permissions. The encryption solution can be built in or 3rd party solution needs to be factored to meet the requirement. **Priority : (D-Desired)**
37	Page no 13/ Aneex-II	Security Awareness Training: Integration with security awareness training platforms to educate employees on data protection best practices. **Priority : (M-Mandatory)**	Security Awareness Training: Integration with security awareness training platforms to educate employees on data protection best practices **Priority : (D-Desired)**
38	Page no 13/ Aneex-II	Policy-based Encryption: Automatic encryption of sensitive data based on predefined policies, regardless of its location or format. **Priority : (M-Mandatory)**	Policy-based Encryption: Automatic encryption of sensitive data based on predefined policies, regardless of its location or format. The encryption solution can be built in or 3rd party solution needs to be factored to meet the requirement. **Priority : (D-Desired)**
43	Page no 13/ Aneex-II	Data Masking for Development: Data masking techniques to anonymize sensitive data in development and testing environments.	The system should support incremental scanning during discovery to reduce volumes of data to be scanned.
45	Page no 13/ Aneex-II	Mobile Application Containerization: Isolation of sensitive data within secure containers in mobile applications to prevent data leakage. **Priority : (M-Mandatory)**	Mobile Application Containerization: Isolation of sensitive data within secure containers in mobile applications to prevent data leakage. **Priority : (D-Desired)**

46	Page no 13/ Aneex-II	Data Obfuscation: Techniques to obfuscate sensitive data for specific use cases, such as data analytics or research purposes.	The DLP solution should support as an API be able to provide the risk adaptive based protection by dynamically calling the action plan based on the Risk in future if required.
48	Page no 14/ Aneex-II	Encryption Key Lifecycle Management: Full lifecycle management of encryption keys, including generation, rotation, storage, and revocation. **Priority : (M-Mandatory)**	Encryption Key Lifecycle Management: Full lifecycle management of encryption keys, including generation, rotation, storage, and revocation. The encryption solution can be built in or 3rd party solution needs to be factored to meet the requirement. **Priority : (D-Desired)**
50	Page no 13/ Aneex-II	Integration with Cloud Access Security Brokers (CASBs): Integration with CASB solutions to extend DLP capabilities to cloud applications and services. **Priority : (M-Mandatory)**	Integration with Cloud Access Security Brokers (CASBs): Integration with CASB solutions to extend DLP capabilities to cloud applications and services. **Priority : (D-Desired)**
51	Page no 13/ Aneex-II	Deep Learning for Threat Detection: Utilizing deep learning algorithms to detect and prevent advanced threats, including zero-day attacks.	The 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.
52	Page no 13/ Aneex-II	Security Incident Response Orchestration: Automated orchestration of incident response actions across multiple security systems and tools. **Priority : (M-Mandatory)**	Security Incident Response Orchestration: Automated orchestration of incident response actions across multiple security systems and tools. **Priority : (D-Desired)**
53	Page no 13/ Aneex-II Compliance of Specifications of Data Loss Prevention (DLP) Solution.	Blockchain-based Data Integrity: Utilizing blockchain technology to ensure data integrity and tamper-proof audit trails.	The solution shall ensure data integrity and tamper-proof audit trails.

55	Page no 14/ Aneex-II	Data Classification Labeling: Applying visible labels or watermarks to classified sensitive data to raise awareness and prevent mishandling or unauthorized access. **Priority : (M-Mandatory)**	Data Classification Labeling: Applying visible labels or watermarks to classified sensitive data to raise awareness and prevent mishandling or unauthorized access. **Priority : (D-Desired)**
56	Page no 14/ Aneex-II	Data Loss Prevention for Cloud Storage: Monitoring and controlling data transfers to and from cloud storage platforms, ensuring data security in cloud environments. **Priority : (M-Mandatory)**	Data Loss Prevention for Cloud Storage: Monitoring and controlling data transfers to and from cloud storage platforms, ensuring data security in cloud environments **Priority : (D-Desired)**
59	Page no 14/ Aneex-II	Advanced Threat Intelligence Feeds: Integration with external threat intelligence feeds to stay updated on the latest threats and indicators of compromise. **Priority : (M-Mandatory)**	Advanced Threat Intelligence Feeds: Integration with external threat intelligence feeds to stay updated on the latest threats and indicators of compromise **Priority : (D-Desired)**
61	Page no 14/ Aneex-II	Secure Remote Wiping: Remote wiping of sensitive data from lost or stolen devices to prevent unauthorized access. **Priority : (M-Mandatory)**	Secure Remote Wiping: Remote wiping of sensitive data from lost or stolen devices to prevent unauthorized access. **Priority : (D-Desired)**
66	Page no 14/ Aneex-II	Data Anonymization: Techniques to anonymize sensitive data while preserving its usefulness for analysis, research, or other purposes.	The 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.
68	Page no 14/ Aneex-II	Database Encryption and Transparent Data Encryption: Encryption of sensitive data within databases and transparent encryption of data at the storage level. **Priority : (M-Mandatory)**	Database Encryption and Transparent Data Encryption: Encryption of sensitive data within databases and transparent encryption of data at the storage level. The encryption solution can be built in or 3rd party solution needs to be factored to meet the requirement. **Priority : (D-Desired)**

70	Page no 15/ Aneex-II	Secure DevOps Integration: Integrating data protection controls and security practices into the DevOps process to ensure secure application development and deployment. **Priority : (M-Mandatory)**	Secure DevOps Integration: Integrating data protection controls and security practices into the DevOps process to ensure secure application development and deployment. **Priority : (D-Desired)**
80	Page no 15/ Aneex-II	The solution should support the templates for detecting the Deep Web Urls- .i2P and .Onion , Encrypted attachments to competitors , Password Dissemination , User Traffic over time , Unknown Encrypted File Formats Detection. The solution should support detection of PKCS #12 files (.p12, .pfx) that are commonly used to bundle a private key with its X.509 certificate.	The solution should support Encrypted attachments to competitors, Password Dissemination, Unknown Encrypted File Formats Detection. The solution should support detection of PKCS #12 files (.p12, .pfx) that are commonly used to bundle a private key with its X.509 certificate.
82	Page no 15/ Aneex-II	Data Loss Prevention for Voice and Video Communication: Ensuring secure handling of sensitive data during voice and video calls, including encryption and access controls. **Priority : (M-Mandatory)**	Data Loss Prevention for Voice and Video Communication: Ensuring secure handling of sensitive data during voice and video calls, including encryption and access controls. **Priority : (D-Desired)**

General Terms and Conditions:

Ext. Cl.	Name of Item with page no	Existing General Terms and Conditions as per Tender Schedule	Amendments
9	**Availability of Tender Schedule**	The tender schedule will be available at Procurement of Computer Hardware and Accessories Department (PCHAD), Operations Wing, IBBPLC, Head office, Yousuf Chamber (9th Floor), 20, Dilkusha C/A, Dhaka during office hours from **19.03.2024 to 22.04.2024 upon payment of Tk.5,000/-** (five thousand) only(nonrefundable) per set in cash.	The tender schedule will be available at Procurement of Computer Hardware and Accessories Department (PCHAD), Operations Wing, IBBPLC, Head office, Yousuf Chamber (9th Floor), 20, Dilkusha C/A, Dhaka during office hours from **19.03.2024 to 07.05.2024 upon payment of Tk.5,000/-** (five thousand) only(nonrefundable) per set in cash
10	**Dropping of Tender Schedule**	The tender documents shall be dropped in the tender box to be kept at Procurement of Computer Hardware and Accessories Department (PCHAD), Operations Wing, IBBPLC, Head Office, Yousuf Chamber (9th Floor), 20, Dilkusha C/A, Dhaka latest by **03.00 PM on 23.04.2024**. No tender shall be entertained after the specified time and date. Tender papers must be properly filled in, sealed and signed by authorized official with tenderer's name, address, etc. Only the Technical Offer will be opened at **03.15 PM on same day i.e. 23.04.2024** at the same place in presence of Tenderer or their nominated representative (if any).	The tender documents shall be dropped in the tender box to be kept at Procurement of Computer Hardware and Accessories Department (PCHAD), Operations Wing, IBBPLC, Head Office, Yousuf Chamber (9th Floor), 20, Dilkusha C/A, Dhaka latest by **03.00 PM on 08.05.2024**. No tender shall be entertained after the specified time and date. Tender papers must be properly filled in, sealed and signed by authorized official with tenderer's name, address, etc. Only the Technical Offer will be opened at **03.15 PM on same day i.e. 08.05.2024** at the same place in presence of Tenderer or their nominated representative (if any).

17/04/24
Officer (PCHAD)

17/04/24
SO (PCHAD)

17.04.2024
FAVP (PCHAD, OW)

17.04.2024
AVP & Head of PCHAD, OW