# ISLAMI BANK BANGLADESH LIMITED

OPERAIONS WING, ENGINEERING DIVISION
PROCUREMENT OF COMPUTER HARDWARE
AND ACCESSORIES DEPARTMENT
20, DILKUSHA C/A (9th Floor), DHAKA – 1000.

**Annexure-A**

## NOTICE INVITING TENDER FOR PROCUREMENT OF 2001 ANTIVIRUS SOFTWARE USER LICENSES OF McAFEE COMPLETE ENDPOINT PROTECTION– BUSINESS SUITE (CEB) FOR WINDOWS.

Sealed Tenders are hereby invited by Islami Bank Bangladesh Limited from reputed Manufacturers / Local Agents / Companies / Dealers / Authorised Distributors for **procurement of 2001 Antivirus software user Licenses of McAfee Complete Endpoint Protection– Business Suite (CEB) for Windows** of Islami Bank Bangladesh limited under the following terms and conditions:

| Item | Brand & specification | Quantity | Remarks |
|---|---|---|---|
| **Antivirus software user Licenses for windows** | **McAfee Complete Endpoint Protection– Business Suite (CEB)** | **2001** | **For 3 years;** |

**N.B.: Offers to be submitted as per tender schedule;**
Brief specification of the item is as under:

| Sr.No | Features | Compliance |
|---|---|---|
| **A** | **AV protection for Desktop and Servers** | |
| 1 | Solution must provide Virus protection at Servers and Desktop level | |
| 2 | Guard all Windows, Mac, and Linux endpoints against system, data, email, web, and network threats | |
| 3 | Solution must provide automated and centralized download and deployment of latest virus signature updates from the Internet to desktops and servers across the organization, across different Windows platforms. Updates should be incremental with update sizes of < 100KB on average | |
| 4 | Antivirus DAT size should be under 100MBs. | |
| 5 | Solution must provide flexibility to install different components (Like – Management Agent, AV client, Anti-Spyware, Device Control, Firewall) separately for better use of network bandwidth | |
| 6 | Should have the ability to detect and remove unwanted joke programs, toolbars, adware, spyware, dialers etc& Post detection the actions that the antiviral performs must be the following: | |
| 7 | Alert / Notify , Clean, Delete / Remove, Move / Quarantine, Prompt for Action | |
| 8 | Shall support multiple Windows platforms | |
| 9 | Endpoint protection must have scored the highest in a test of protection against evasion attacks in 2013 NSS Labs report. | |
| 10 | Should support file scan caching to avoid repetitive scanning of files which are unchanged since the previous scan | |
| 11 | Proposed solution must automatically scan Compact disks, USB devices and Network shares in real-time when accessed. | |
| 12 | Proposed solution should provide multiple policies to lockdown the desktop like – change in registry, Internet Explorer file settings, Exe file execution etc to block unknown zero day attacks and reduce dependency on frequent signatures | |
| 13 | Should allow the On Demand Scanner to recognize the last scanned file and resume scanning from that file if an "On demand Scan" is interrupted | |
| 14 | Should have the ability to control the amount of CPU resources dedicated to a scan process | |
| 15 | The proposed solution should be capable of detecting and preventing buffer overflow vulnerability, irrespective of the exploit that is using the buffer overflow vulnerability. The solution should support buffer overflow detection and prevention on the following minimum applications: | |

| | | |
|---|---|---|
| 16 | Windows OS Services, Media Player, Internet Explorer, SQL Server, Word, Excel, Power Point, Auto Update, Explorer, Instant Messenger, Outlook, Outlook Express etc | |
| 17 | Proposed solution should be capable of blocking TCP/IP ports on the System and also creating exceptions for specified applications to use these blocked ports. | |
| 18 | Proposed solution should be capable of blocking read, write, execute, delete & change permissions on specified file(s)/folder(s)/Network Share(s). | |
| 19 | The proposed solution should provide Self-protection from modifying or disabling VirusScan Enterprise | |
| 20 | The management server should have a database which supports merging, backups, restoration and replication | |
| 21 | Should support protection against POTENTIALLY UNWANTED PROGRAMS | |
| 22 | Proposed solution should have integrated URL categorization feature | |
| 23 | Should have Web Filtering for Endpoint as an optional add-on module that provides secured web access for anyone using the Internet for work-related or personal business—in or out of network. | |
| 24 | Proposed solution should categories URLs for threats like – Spywares, Trojans, Spam, Adwares, Red links | |
| 25 | Solution URL category module should provide end user detail threat information about the site | |
| 26 | The proposed solution should scan system memory for installed rootkits, hidden processes, and other behavior that suggests malicious code is attempting to hide itself | |
| 27 | The proposed solution should allow to configure different policies for different set of Processes | |
| 28 | Guard all Windows, Mac, and Linux endpoints against system, data, email, web, and network threats | |
| 29 | Should be able to lock down all anti-virus configurations at the desktop | |
| 30 | Proposed solution should be capable of detecting and blocking communication from hosts that are spreading viruses/worms. | |
| 31 | Proposed solution must identify machines plugged into the network and notify the administrator of the presence of a machine without an Antivirus engine running on it. | |
| 32 | Buffer overflow protection exclusions by API | |
| 33 | Heuristic network check for suspicious files | |
| 34 | Protection from malware even if no signature file available locally | |
| 35 | The proposed solution must be in Gartner's leader's quadrant for atleast last 3 years. | |
| 36 | Should have enhanced tamper protection that guards against unauthorized access and attacks, protecting users from viruses that attempt to disable security measures | |
| **B** | **Antivirus and Anti-Spam for Mail Server (Exchange / Domino)** | |
| 1 | It should scan all mails passing through the Mail Server and cure for infections in documents attached to email messages and folders | |
| 2 | The real-time monitor should scans for viruses while messaging systems are live and running—without disturbing users | |
| 3 | It should support heuristic scanning for viruses and worms for which signatures are not released and documented | |
| 4 | Infection treatment should support report-only, cure, delete, move and rename file | |
| 5 | It should allow to pre-define certain extensions which can be blocked/exempted even without scanning | |
| 6 | It should allow scanning specified extensions or exclude certain extensions and allow scanning various types of compressed files | |
| 7 | It should allow notifications being sent to the owner, sender and administrator when and infection is detected | |
| 8 | Spam Prevention based on a search in the email body, header & attachments | |
| 9 | Spam prevention based on a pre-defined spam dictionary White List for trusted mail server, relays, email users and domains for a configurable time | |

| | | |
|---|---|---|
| 10 | Attachment type recognition based on attachment extension, content, file type or file name | |
| 11 | Should search for keywords in the message content and block and alert the administrator in case found | |
| 12 | Facility of blocking e-mail addresses from where we do not want to receive e-mails | |
| 13 | Filters should automatically be downloaded from the proposed solution vendor to customer | |
| 15 | It should allow scanning the message body and supporting exchange features like proactive scanning and background scanning | |
| 16 | It should be possible to specify the number and level of detail of logs to keep | |
| **C** | **Enterprise Anti-Spyware** | |
| 1 | Must be able to totally protect from spyware, adware, Trojans, key loggers, P2P Threats, Hackers tools, DDOS Attack Agents, in real time | |
| 2 | Must be able to support Interactive scan on demand | |
| 3 | Should have centralized management and reporting capabilities to deliver reports like top Spywares, by category, by infected machines, by risk priority etc | |
| 4 | Real time Active protection on memory, process termination / file removal of pests in active memory | |
| 5 | Must be able to scan from the desktop according to preset or customized configurations | |
| 6 | Should have centralized update/download mechanism which should be able to download details of latest Spywares and push the same across all the desktops | |
| 7 | The solution must be able to auto-quarantine or auto-delete spyware or adware without end-user interaction | |
| **D** | **Management & Reporting** | |
| 1 | Proposed solution should provide single console to manage or integrate with the present or any components required in future like | |
| | Anti-Virus | |
| | Anti-Spyware | |
| | HIPS | |
| | Desktop Firewall | |
| | Mail Server AV | |
| | SMTP AV | |
| | Spam Prevention | |
| | Policy Auditor | |
| | Data Loss Prevention | |
| | Network IPS | |
| 2 | Management console should have capability to ask real time questions and take actions on response in real time. It should not reply on logs to give real time visibility of security environment. The analysis should happen on all client machines when queried and not analyzed by logs of management system. | |
| 3 | The management tool should provide support for Microsoft Clustering Services. This would ensure that the management server is always available, even if the primary server shuts down for any reason | |
| 4 | The centralized management console may be web-based | |
| 5 | The centralized management console should be capable of deploying remotely the managed products (such as desktop AV) on a machine | |
| 6 | The tool should support hierarchical grouping of machines and policy deployment. The grouping could be based on IP Address of a subnet of machines or a particular site | |
| 7 | The Centralized management tool should be capable of deploying Pattern Files, Scan Engines, emergency releases of pattern files, patches, hot fixes and new product versions for all managed products | |
| 8 | The centralized management tool should be able to deploy signature files for different products | |

| | | |
|---|---|---|
| 9 | Centralized management console should provide dashboard with multiple information & these information should also be fetched from database based on different queries | |
| 10 | Console should support tagging of information in the database to provide flexible reporting | |
| 11 | Administrator should be able to configure the update process as automatic or manual, controlled deployment | |
| 12 | Update process should conserve WAN Bandwidth by having a distributed framework for signatures and policy updates | |
| 13 | The centralized management console should provide management reports for different managed components like – Top N reports, Trend reports, Outbreak reports, Compliance reports, | |
| 14 | The centralized management console should support the way to build custom queries on the database to create custom reports | |
| 15 | Central management console should provide automatic generation and delivery of reports to the respective administrators | |
| 16 | Central management console should provide actionable reports | |
| 17 | Central management console should support granular role based access control | |
| 18 | The Centralized Management Console should deliver security threat information including current threats and the DAT and engine files necessary to protect against them | |
| 19 | Must have the policy to restrict or permit access to potentially harmful web sites. | |
| 20 | Site Advisor Solution should warn employees before they interact with dangerous web sites, and give them the freedom to search and surf online with protection from web-based threats. | |
| 21 | Prevent disruption and downtime from rogue systems that do not have agent installed by being able to identify them as they connect to the network | |
| 22 | Policy sharing across servers and roll-up reporting | |
| 23 | Should support agent handlers to allow management of end systems ,even off the network | |
| 24 | Management server should correlate threats, attacks, and events from endpoint, network, and data security as well as compliance audits to improve the relevance and efficiency of security efforts and compliance reports. | |
| 25 | Proposed Solution should be Recognized for four straight years by Gartner as a leader in Endpoint Security and Mobile Data Protection | |
| 26 | The software should use a scalable peer-to-peer methodology for querying information from all the endpoints in mere moments, with no extra hardware | |
| 27 | Solution should reduce the cost of managing IT security and compliance by more than 60 percent based on survey by agencies like MSI International of more than 450 mid-sized and large enterprises). | |
| 28 | The management server should be able to manage/report other vendors' products too | |
| 29 | Management server should have Real-time /instant visibility of security threats ,should have an option of asking questions to get real-time status. | |
| **E** | **Application Control** | |
| 1 | The Solution should ensure that Only authorized software / applications / executable codes are allowed to run and provides tamper protection to them. | |
| 2 | Solution should be capable of creating white list for each system dynamically and no manual intervention in creating this list. | |
| 3 | Each white list created should be unique to each system and should not be a common list | |
| 4 | The solution should emper the user to self-approve any new application / software with business justification. So that new application can be run successfully with notification to administrator. | |
| 5 | Solution should allow administrator to approve or revoke self-approved application status so that new application can be allowed to run or ban. | |
| 6 | Solution should consider executables, activeX, Java, Perl scripts, bat files, VBS files, com files, dll files, sys files while creating the white list. | |
| 7 | Solution should be capable of locking down the system on the white list created above and prevent execution of non white listed software / application / executable code. | |

| | | |
|---|---|---|
| 8 | Solution should prevent tampering of applications which are white listed above either on disk or on memory when running | |
| 9 | The Solution should have the capability to run on observation mode post white list creation so that new applications / software / codes are not stopped from running but are monitored only. If required administrator should be able to approve or revert back to base line. | |
| **F** | **MDM** | |
| 1 | Should have a Mobile Device Management product | |
| **G** | **Hardware Assisted Security** | |
| | Should have a product to blocks stealth attacks with hardware assisted security approach | |
| **H** | **Host IPS** | |
| 1 | Should have HIPS with FW | |

**Detail specification mentioned in the Tender document.**

## Terms and Conditions:

**01.** The intending Bidders have to apply in their letter head pad for purchasing of tender Document and document will be sold to the intending bidders from Procurement of Computer Hardware and Accessories Department, ED, HO, IBBL, 20 Dilkusha, Yousuf Chamber (9th floor) during Office hours from **19.01.2016 to 27.01.2016** upon payment of **Tk.5,000.00 in cash (non refundable)**. No Tender document will be issued/ received by mail.

**02.** Tenders will be received at the office of the undersigned up to **3.00 PM** on **28.01.2016** and Technical offer will be opened at **3.10 PM** on the same date and same place that is in the office of the undersigned in presence of the bidders who may like to attend to the tender opening meeting. After completion of technical evaluation, financial offer of the qualified bidders will be opened through informing the same to the participating bidders.

**03.** 2.5% (two point five percent) of the total tender amount must be submitted along with the tender in favour of Islami Bank Bangladesh Limited in the form of Bank Draft/ Pay Order/ Bank guarantee from any scheduled Bank of Bangladesh preferably from Islami Bank Bangladesh Limited without which the Tender shall be rejected outright.

**04.** An original and one copy of the Offer duly marking **"Original Offer_Technical"** and **"Copy of the Offer_Technical"** and **"Original Offer_Financial" and "Copy of the Offer_Financial"** should be submitted at the time of tender submission with authentication by the Tenderers. **Combination of Technical and Financial Offer will be disqualified.** The bid form must be filled in through computer printer or in typing without overwriting and without any erasing and modifications and when completed shall contain all the required information.

**05.** Islami Bank Bangladesh Limited reserves the right to accept any tender and reject any or all tenders without assigning any reason whatsoever. Islami Bank Bangladesh Limited is not bound to purchase the item from the lowest bidder.

## Senior Vice President