THE ANDHRA PRADESH STATE CO-OPERATIVE BANK LTD.

(Govt. Partnered Scheduled Bank)
HO: NTR Sahakara Bhavan, # 27-29-28, Governorpet, Vijayawada-520002
Information Technology Dept. : Email-id: info.tech@apcob.org

RFP Ref. No.: APCOB/IT/F.99 Antivirus/2023 Date: 25.04.2023

SHORT TENDER NOTICE

Supply and installation of Enterprise Endpoint Security Solution (K7 Anti virus) in APCOB

1. Preface

The Andhra Pradesh State Co-operative Bank Limited (APCOB) is a Govt. partnered scheduled Bank working with its Head Office in Vijayawada and 18 Branches. The Bank is planning to procure Enterprise Endpoint Security Solution in APCOB

2. Objective of the RFP:

APCOB is issuing this Request for Proposal Document, hereinafter called as a Tender, to vendors who are eligible to participate in the competitive Tendering for supply and installation of Enterprise Endpoint Security solution (K7 Antivirus) in APCOB.

3. Scope of Work:

Supply and installation of Enterprise Endpoint Security Solution in APCOB

The broad scope of work is given below: -

TECHNICAL SPECIFICATIONS

ENDPOINT SECURITY SOLUTION (read as EPS)	
1	EPS must be Enterprise Endpoint Security Version
2	EPS must offer comprehensive client/server security by protecting enterprise networks from viruses, Trojans, worms, hackers, network viruses, mixed threat attack from multiple entry points, and spyware.
3	EPS should have the capability to detect all in-the-wild viruses and Antivirus Engine; OEM should have their own engine and should be certified with reputed VB100%, AV Comparative and AV Test
4	EPS OEM should have their OWN ENGINE and should be certified with any one of the reputed testing bodies like VB100%, AV Comparative, AV Test
5	EPS should support or future ready to support multi-platform OS through single/ multiple consoles if there is need in department.
6	EPS should support or future ready to support Mobile device management through single/ multiple consoles if required.
7	EPS Should support Windows XP SP1/SP2/SP3 and should work even on low end configuration machines
8	EPS must have the capability to detect and block files with malicious executable content and embedded/compressed executables that use real-time compression algorithms.
9	EPS must have the capability to detect and remove rootkits.
10	EPS must have the capability to Schedule/run task to remove root kits from Administrator end.
11	EPS must have the capability to detect and quarantine suspicious files.
12	EPS must have the capability to detect malware by behavioural detection techniques.
13	EPS must have the capability to detect and remove rogue wares.
14	EPS must have the capability to identify source of infection i.e. from where the infection has originated in the network.
15	EPS must have the capability to restore a file from quarantine if the file is deemed safe.

16	EPS must provide Virus Outbreak Prevention mechanism, which should be acted based on threshold of detected malware.
17	EPS Should have anti malware protection and clean up capability.
18	Ordinary users should not be able to modify AV settings or uninstall the EPS through OEM removal Tool.
19	EPS should allow administrators to make changes in AV enable/disable, Firewall enable/disable & uninstall EPS through console.
20	EPS OEM should have the capability to block any third party .exe removal tools for uninstalling endpoint security.
21	Update Managers: Should have the capability to create multiple update servers to distribute updates load in large network environment that reduce bandwidth consumed during definition updates.
22	EPS must have the capability to perform different scan actions based on the virus type (Trojan/ Worm, Joke, Hoax, Virus, other)
23	EPS must have the capability to scan compressed, archived, and packed files.
24	EPS must have the capability to scan plug and play USB storage drives as soon as they are connected.
25	EPS must have the capability to terminate virus program threads in memory, repair registry, remove any malicious OS processes created by Trojans.
26	EPS must protect from any new viruses and threads in future.
27	EPS must have the capability to scan and repair OLE (Object Linking and Embedded) files.
	ADD ON SERVER
1	EPS must have the capability to improve performance of endpoints by cleaning junk files and deleting invalid registry/disk entries.
2	EPS must have the capability to manage mobile workforce when they moves out of the corporate network.
3	EPS must have the capability to identify and report vulnerabilities of installed applications and operating systems in the network.

4	Bidder or vendor should have provided MAF from OEM.
5	EPS should support add on server architecture.
6	The location of Add on server, on which add on will be updated, will be decided by concerned department or administrator
7	The necessary Hardware will be provided by department.
8	The Add on server will be configured as per requested locations.
9	Add on server shall be capable of fetching update from central location through WAN And distributing the same over LAN.
	DEVICE CONTROL
1	EPS must have the capability to grant allow, block, read-only access to various storage devices.
2	EPS must have the capability to grant access rights for storage devices such as USB, CD/DVD, Card Reader, etc.
3	EPS must have the capability to regulate the use of Wi-Fi and Bluetooth connections.
4	EPS must have the capability to retain control over interfaces such as Fire wire Bus, Serial Port, SATA Controller, Thunderbolt, etc.
5	EPS must have the capability to control and regulate the use of printers, scanners, web cameras, and network shares.
6	EPS must have the capability to exclude any particular device from device control policies.
	TEMPORARY ACCESS TO USB DEVICES
1	EPS should be capable to give temporary access to USB storage devices enables administrators to give access of USB devices for some particular period even if the Device Control policy is set to block.
2	EPS should allow USB devices with specified Model Name can be excluded in Device Control Policy.
3	Blocking complete USB Interface will deny access to USB devices such as USB dongles, USB Cameras, USB scanners etc. (except Input devices such as Keyboard, Mouse)

4	EPS should also have device Control which supports NTFS and FAT drive for authorization
5	EPS must have the capability to exclude certain files/folders/paths from monitoring/scanning procedures.
	ASSET MANAGEMENT
1	EPS must have the capability to collect system and hardware information related to remote endpoints.
2	EPS must have the capability to obtain a summary report of various software's/updates installed on endpoints.
	APPLICATION CONTROL
1	EPS must have ability to add custom applications to the blocked application list.
2	EPS must have capability to collect list of all installed applications in the network.
	ROAMING PLATFORM
1	Roaming service allows interacting with EPS server when the clients are outside the organizational network. This allows the administrator to apply the policies, installation, if required
	IDS/IPS
1	EPS must have the capability to detect, and prevent network based and host based intruder attempts on the home networks.
2	EPS must have the capability to prevent port scanning attacks.
3	EPS must have the capability to prevent DDOS attacks.
4	EPS must have the capability to generate reports for potential security breaches, policy violations, and suspicious traffic flow.
	WEB SECURITY AND WEB FILTERING
1	EPS must have the capability to block user access to malicious and phishing websites from configured endpoints.
2	EPS must have the capability to block user access to websites based on their categories e.g. Social Networking, News, etc.

3	EPS must have the capability to block entire domain or a particular website/URL
4	EPS must have provision to exclude certain websites or entire domains.
5	EPS must have the capability to block https sites.
	PATCH MANAGEMENT
1	EPS should allow administrator to generate exhaustive reports on system vulnerabilities, patches, OS, etc
2	EPS should not push updates automatically but allow the admin to prioritize and update manually.
	DATALOSS PREVENTION
1	EPS must have capability to enable password protection for removable /external storage devices.
	FIRE WALL
1	EPS must have on desktop or soft firewall for additional
2	EPS must provide the flexibility to create firewall rules to filter connections by IP address, port number, or protocol, and then apply the rules to different groups of users.
3	EPS must have the capability to examine and control all incoming and outgoing traffic per configured settings for ports, source, or origin or destination address.
	EMAIL PROTECTION
1	EPS must have the capability to create multiple user groups as per organizational structure.
2	EPS must have the capability to assign different policy configuration to each group.
3	EPS must have the capability to import/export groups and policies.
4	EPS Must provide Policy deployment status (Applied, Pending or Failed) on EPS web console
	CLIENT DEPLOYMENT
1	EPS must have the capability to deploy the Client software using the following mechanisms:

2	EPS should have Client Packager (Executable & Microsoft Installer (MSI) Package Format).
3	EPS should have Web install page/package
4	EPS should be capable of pushing remote installation on single end point or on entire IP range.
5	EPS should be capable of installing through Active Directory and by creating group policy object
6	Client uninstallation should only be done by administrator
	MANAGEMENT FEATURES
1	EPS must provide a secure GUI or Web-based management console to give administrators access to all clients and servers on the network for client administration.
2	EPS must have the flexibility to roll back updates if required.
3	EPS Should have role based administration capability.
4	EPS must support plug-in modules designed to add new security features without having to redeploy the entire solution, thereby reducing effort and time needed to deploy new security capability to clients and servers across the network
5	EPS web console should support on Google Chrome, Internet Explorer and Mozilla Firefox Browsers and all browsers available in the network.
	NOTIFICATION, REPORTING AND LOGGING
1	EPS should provide email notification for various critical events such as virus outbreak, license getting expired etc..,
2	EPS must have the capability to generate graphical as well as tabular reports.
3	EPS must have capability to export reports in multiple formats such as PDF and CSV.
4	EPS must have capability to automatically send the report to administrators email address as per configured schedule.
5	EPS must have capability to automatically purge old reports after a preconfigured duration.

6	EPS must have capability to log activities of management server.	
	OTHER REQUIREMENTS	
Upgrade and Updates	EPS software solution should be quoted with three years upgrade & updates subscription.	
License	The antivirus software should be licensed to APCOB for three years, with an enterprise edition.	
Training	An in-house training of minimum 6 hrs. to IT officials of APCOB and FMS team for day-to-day operation and maintenance of the antivirus is to be given by the selected bidder.	
Antivirus Management Services	The company will arrange a visit of Technical professional every month, who would do random check of the Servers and will give a report of inspection regarding satisfactory working of antivirus.	
Installation Period	The entire installation to be completed within 45 days from the issue of Letter of Acceptance/ Purchase Order.	
	INSPECTION	
	APCOB shall have the right to inspect or to test the product to confirm their conformity to the ordered specifications. The successful bidder shall provide all reasonable facilities and assistance to the inspector at no charge to APCOB. In case any inspected or tested products fail to conform to the specifications, APCOB may reject the same and successful bidder shall replace the rejected product with the products in conformity with the specification required free of cost to APCOB. Any delay due to above shall attract relevant penalty clauses of the tender.	
	PROJECT TIMELINESS	
	A time of 7 days will be given from the start of the contract period for completing the project.	
	Placement of Purchase Order (PO)	1 Day
	Acceptance of PO	1 DAY
	Signing of contract	5 DAYS
	Supply, Installation, Configuration of Products/Licenses and Commissioning of the services	7 DAYS

	Stabilization and issuance of Acceptance Certificate by APCOB	30 DAYS
	RESPONSIBILITY OF BIDDER	
	Installation, Configuration Commissioning of Software. Submission of Invoice with proper relevant documents.	

4. **Consolidate Requirement:**

S. No.	Name of Work	Quantity
1.	**Enterprise End-point protection suite with web-based administrator console and clients with 3yrs (36 Months) support**	**100 Nos**

Other Terms and Conditions:

- Rate contract will be on Base Unit
- The Rate contract will be for a period of 1 year from the date of the Purchase Order.
- Total cost inclusive of all taxes, service tax, and surcharge, if any, to be indicated.
- 100% Payment shall be made after completion of work and upon the submission of invoice along with the work completion report.

Eligibility Criteria:

1. The bidder must be a Registered Company and having its operations for a minimum period of 3 Years and bidder may be MSME/Registered firm/LLC.
2. Average Annual financial turnover during the last / Previous 3 years ending 31st March of 2023 should not be less than 10 Lakhs.
3. Bidder must have its own valid PAN No. and GST Registration No. TIN & CIN registered in the state of Andhra Pradesh.
4. The bidder must submit Manufacturing Authorization form (MAF).

Schedule:

Tender Reference Number	APCOB/IT/Hardware/Date:25.04.2023
Last Date for Submission of Proposal	Date and Time: 27.04.2023 and 4:00 PM
Opening of tenders	Date and Time: 27.04.2023 and 04:30 PM

Website to Download the requirements	https://www.apcob.org/
Contact Person at APCOB	M S R G Tilak Nara. Deputy General Manager Email: info.tech@apcob.org Contact No: 08662429036

Sd/-
M S R G Tilak Nara.
Deputy General Manager