JANATA SAHAKARI BANK LTD., SATARA.

Owner	**Janata Sahakari Bank Ltd., Satara.**
Date	**11th October 2023**

Table of Contents

Request for Proposal for Endpoint Protection Solution

1 Overview of Requirements

As a part of the technological process & Security purpose Bank is planning to procure **(A) Enterprise level endpoint protection solution** and also **(B) implementation of Active Directory** (the specifications, scope of which are mentioned in Sr. No. 6 under "Technical Specifications" below) for its Head office and branch offices from the qualified and reputed firm/companies on the following terms and conditions.

2 Instructions to bidders

This covers following parts

1) Tender form will be evaluated in two parts
    a. Commercial for item (A) and (B)
    b. Technical for item (A) and (B)
2) Bidders need to provide Commercial Bid for item (A) and (B) in a separate sealed envelope.
3) Only those vendors, who are able to do both the tasks (A) and (B) should submit the quote and who are able to meet the specifications, features, scope mentioned in the tables (A) and (B) stated under Sr.No.6 under 'Technical Specification' should submit the Bid.
4) As regards to item (A) i.e. Endpoint protection solution, the bidders need to submit the quote for 50 user licenses with 3 years subscription. The solution should be scalable to increase/extend more number of users in future as per the requirement of the Bank.
5) Bank will consider the quote from single vendor, who has submitted bid for both the items (A) and (B) only. Please note that Bid for any of the single item will not be entertained and will not be considered.
6) Bidders need to provide Technical Bid in a separate sealed envelope with the followings:
    a. Covering Letter
    b. Additional information if any
    c. Brochure
7) **OEM Authorization** letter to be provided in the Name of the Bank.
8) The vendor will be responsible for the successful installation of the endpoint solution product at the various locations of the branches and offices of the bank as per the requirement of the Bank. As regards to Active Directory implementation, the vendor is responsible for completion of all the tasks and related activities, polices like grouping of entire computer system, network, active directory, configuration as per requirement of the bank, in coordination with other vendors of the

Bank. Bank will not provide any extra cost for implementation of both the items.

3 Submission of BID:

- The vendor should submit the BID document in the format mentioned below under serial number 7 “Commercial Bid Format” , in a sealed envelope as mentioned above **By Hand only** at the below address of the Bank :
- Address of Bank: Head Office, 179, Bhavani Peth, Rajpath, Satara.-415002.
- Last Date & Time of Submission of BID: 20/10/2023 upto 5:30 pm.

4 General:

- The Bank reserves the right to reject any or all the tenders, or call off the entire tender process without providing any specific reason.

5 Evaluation

The evaluation of the bidders will be done on the basis of criteria mentioned below.

- Bank will consider the quote from single vendor, who has submitted bid for both the items (A) and (B) only. Please note that Bid for any of the single item will not be entertained and will not be considered.
- The vendor should be direct partner of OEM (Original Equipment Manufacturer).
- The main factor of selection will be meeting the technical requirements, quality and local infrastructure of the vendor for after sales support.
- The timely delivery of the product solution will be one of the criteria of the evaluation.
- Finally the Price, Performance/Return on Investment, post sales service, experience of the vendor will be important factors for finalization.

6. Technical Specifications:

The enterprise security solution should comprise of comprehensive, integrated, layered endpoint protection solution that should deliver the real-time visibility, analysis, protection and remediation for endpoints. It should be combination of advanced and futuristic technologies that provides protection to Windows, Mac, Linux, iOS and android based devices and endpoints in the Bank's Network and must have following features, but not limited to.

- Web Interface with Dashboard
- Asset Management
- Data Leak Prevention Attachment Control
- Detailed technical specifications are mentioned in the below table:

Sr. No.	A) Technical specifications for Endpoint Protection Solution 50 user licenses with 3 years subscription.
1	Solution should have unique scanning and detection technology for Malwares and dedicated engine for Ransomware detection and blocking
2	Proactive Scanner with AI and Machine Learning Capabilities
3	Solution should have intelligent self-protection
4	Solution should have real-time Email Scanner at endpoint
5	Should be able to protect against Key-logger , File-less Malware , Root-kits, Spyware, Ransomware and Zero-day attacks and should be EDR compliant.
6	solution should have real-time file monitor with EDR capabilities.
7	The solution must block fileless attacks, exploitation behaviour, Ransomware using IOC.
8	The solution must identify malicious behaviour of executed files\running processes\registry modifications\ memory access and terminate them at runtime, or raise an alert (exploits, file-less, Macros, PowerShell, WMI etc.).
9	The solution must support the creation of rules to exclude files based on hash, filename and folders
10	The solution must identify and block/alert on lateral movement
11	The solution must identify user account malicious behaviour, indicative of prior compromise
12	The solution should detect when using file-less and malware-less tools such as PowerShell.
13	The solution must continuously collect data on all the entities and their activities within the environment.
14	The solution must support the display of entity and activity data

15	The solution must support and establish real time response connection to endpoints
16	The solution must have user role for real time response attributes
17	The solution must blacklist hashes through UI
18	The solution must support isolation and mitigation of malicious presence and activity.
19	The solution must include threat hunting
20	The solution must have the ability to enable/disable certain types of notifications
21	The solution must have the ability to rate the severity of security alerts
22	The solution must support standardized and customizable reports.
23	The solution must have automatic and configurable out-break prevention
24	Solution must provide complete visualization of attack
25	Solution must provide Automatic as well as Manually Root cause analysis
26	Solution must provide terminal service protection module with configuration of subnet as well as Foreign traffic.
27	solution should have a on demand scanner
28	solution should have Malware mitigation of URLs capabilities with cloud intelligence
29	solution should have capabilities to do fast scanning with technologies based on time saving logics during scans
30	The solution should be able to control access of executable over network.
31	The solution should be able to control access of specific and defined executable on the endpoint.
32	The solution should be able to control self-executing functionality from external devices.
33	solution should have able to detect /block brut force attack over terminal session to the endpoint.
34	The solution should be able to provide controlled access (modification & deletion) of defined folders.
35	The solution should be able to provide controlled access (modification & deletion) of defined files and also based on remote/local users.
36	Gateway Protection at Winsock layer of each endpoint gateway.
37	solution should scan in-coming/Out-Going emails at the client
38	solution should be able to block attachments based on type
39	Solution should have attachments white listing
40	solution should be able to archive emails and attachments
41	solution should be able to take actions on malicious emails based on user defined actions
42	solution should be have customizable alert notifications for various events

43	Solution Should include EDR functionality with respect to handling malicious email content.
44	solution should have a real-time anti-spam engine based on Artificial Intelligence & Machine learning
45	Solution should also include intelligent Anti-Phishing filter
46	Solution should allow customer define phrases to categorize as spam
47	Solution should identify and quarantine advertisement email
48	Solution should be integrated with NILP technology
49	Solution should include email protection sensitivity level to categorize an email as spam.
50	Solution should be able to publish and authorized domain owner list to reduce spam and frauds.
51	Solution should able to integrate with multiple external services which provide databases of malicious content of URLs
52	Solution should also be able to provide auto configuration for white listing of domains.
53	Solution should have strong mail tagging parameters
54	a) Pass the email as it is even if detected as a spam
55	b) Spam tag added in subject
56	c) Intelligent X-mailscan-Spam tagging for subject lines & as header.
57	Solution should have customizable disclaimers.
58	Solution should be able to sent customize notifications or event base alerts.
59	Solution should be able to provide a summarized ham mail reports.
60	Solution should have an intelligent filter configuration to identify Chinese and Korean character set
61	solution should have integrated category base filter for URLS and should be customizable based on an Organization's access policies and culture.
62	solution should have cloud intelligence capabilities for understanding and blocking malicious URLs
63	Solution should able to automatically populate the block category by rejected site.
64	Solution should be able to log policy violations and should be inclusive of EDR function.
65	Solution should have ability to control internet access port
66	Solution should allow the web access on a time grid base policy control mechanism
67	solution should have smart Anti-phishing filter
68	solution should allow port access customizations for Url accesses .
69	solution should be EDR compliant based on log violations
70	solution should include a two way state full intelligent firewall.
71	Solution should have various modes of control intrusive and non-intrusive based on policies.

72	Solution should have zone rules which can be customize based on IP Address segments/Host name/MAC Address.
73	Solution should be able to set complex rules base on Protocol
74	solution should be able to mitigate DDOS attacks & Port Scan
75	solution should be able to provide a network monitoring
76	solution should be able provide all the events in real time and reports of violations
77	solution should have password protection for USB devices
78	solution should be able to block USB Auto play
79	solution should be able to block USB Drives, CD/DVD Drives, web cams, Bluetooth Devices
80	solution should provide a facility of read only mode of USB Storage devices
81	solution should block other modes which can be used for data transfer (for e.g. File transfer from IM's)
82	solution should have complete Application control module with White listing/Blacklisting based on time restrictions
83	solution should have USB Vaccination tools. So that the pen drive doesn't get infected if inserted in a infected machine.
84	solution should be able to block uploading to URL.
85	Solution should have dedicated application control module.
86	Solution should have time-grid base application control.
87	Solution should include white list for company authentic applications.
88	solution should be able to erase temporary internet and windows temporary files
89	solution should be able to clear browser history based on a schedule
90	solution should be able to clear cache , cookies , plug-ins, ActiveX , history on a schedule.
91	solution should have a secure delete function
92	solution should be able to remove temp files , cookies , MRU lists from registry
93	Solution should have capabilities to provide complete inventory of Hardware and software.
94	Solution Should have capabilities to provide Microsoft office & OS license details.
95	Solution should have capabilities to set notification for any hardware and software changes.
96	Solution should have capabilities to monitor create, copy ,modify, delete of file from system to External drives, Network Drives & Local drives
97	Print Activity Monitor
98	Solution should have capabilities to Monitor all the network share printer and provide summary list of all printing activities base on Printer Name/Host Name/Ip address/Document name.

99	solution should be able to manage all the functionality from a centrally managed server via console and on heterogeneous platform (Windows , Linux, Mac)
100	solution should be able to provide a real time dashboard on the status of the Endpoints
101	Solution should be able to provide Application Access Report with detail information.
102	Solution should be able to provide details of Missing windows patches as well as 3 rd party application missing patches
103	solution should be able to provide detailed reports with export facility for all the features and functionalities in various formats (PDF, excel, HTML etc.).
104	solution should be able to provide group based categorization for viewing, policy deployment , task schedule and for complete MIS
105	solution should provide OTP facility for temporary access which should be time based
106	solution should have a Outbreak Prevention task in case of a virus attack
107	solution should have hierarchal administrative role based user creation
108	Solution should be able to provide complete Audit trail
109	solution should be configurable over http and FTP updates to the client
110	solution should be able to integrate with 3rd party CRM via SNMP and have EDR capabilities with 3rd party apps like syslog server and splunk forwarders
111	solution should be able to do bandwidth management with QOS and able to define sizes of the updates
112	solution should be able to provide auto groupings for endpoints functionality which can be integrated into customized setups
113	solution should have Secondary Server Management Option to manage bandwidth consumption in signature updates in low bandwidth environments.
114	solution should have Activity Reporting option to monitor session activity of Client computers (for e.g. Remote session connect / disconnect , Start-up /Shutdown)
115	solution should have module to monitors and logs printing tasks done by managed endpoints.
116	solution should have Backup functionality with encryption. Able to take backup on Local, Network, Google drive, One drive etc..
117	solution should have backup and restore option for AV Server Settings.
118	solution should have a Task Deployment option to disable required modules for short time.
119	solution should have Active Directory Synchronization
120	solution should have “Message Broadcast” option
121	solution should have policy based option to move computers to non-license if not connected for specified number of days.

122	solution should have critical events alerts option. (for e.g. Ransom ware detected, computer moved to unlicensed, new computer detected etc.)
123	solution should have automatic functionality to remove computer from Management Console if AV is uninstalled.
124	With the help of Client Live Updater, events related to Antivirus agent ansd security status of all endpoints are captured and recorded / logged and can be monitored in real-time.
125	Solution should able to provide remotely shutdown , Log off, Hibernate, Restart options for client systems.
126	solution should be able to create a bootable USB with integrated AV toolkit
127	solution should be able to restore default settings
128	solution should have integrated interface to upload virus samples
129	solution should be able to download Windows Essential updates
130	solution should have a registry cleaner inbuilt
131	Should have a rescue mode boot option so that scanning is possible without loading the installed OS
132	solution should have a cloud security network support
133	solution should be password protected on clients.
134	solution should have separate uninstall password.
135	solution should be integrated with remote support client so that OEM can provide quick support
136	solution should be integrated with a data generating input tool which should not be susceptible to key loggers
137	solution should have a DLP function which data can be marked for protection against access and modification over network
138	Solution able to provide Roaming client functionality so user not connect to corporate network will manage from cloud.
139	Solution should able to provide folder level encryption function
140	Solution should be able to Scan in real time for Linux systems
141	Solution should be able to provide On demand scanning function on Linux systems
142	Solution should be able to provide Schedule scan function on Linux systems
143	Solution Should be able to Scan Archive files on Linux systems
144	Solution Should be able to Scan Packed files on Linux systems
145	Solution Should be able to Scan Cross file system on Linux
146	Solution Should be able to provide Application blocking feature on Linux systems
147	Solution Should be able to provide Device control function on Linux system
148	Solution Should be able to provide device whitlisting function on Linux Systems

149	Solution Should be able to provide Password protected USB option on Linux Systems
150	Solution Should be able to provide monitor USB drive functionality on Linux Systems
151	Solution Should be able to provide File integrity monitor on Linux systems
152	Solution should be able to provide category-wise website blocking functionality on Linux Systems
153	Solution Should be able to provide State full firewall on Linux systems
154	Solution Should be able to provide reverse shell white listing/Blacklisting functiion on Linux Systems.
155	Solution Should able to provide Port Scan blocking functionality on Linux systems.
156	Solution Should able to Provide Remote Monitoring Management functionality on Linux Systems
157	Solution should able to provide Asset Management functionality on Linux Systems
158	Solution should provide in build remote support option for taking remote access of systems to technical team.
159	Mobile Device Management
160	Solution should have anti-virus/Malware/Ransomware detection and blocking for mobile devices
161	Solution should scan for files before installations
162	Solution should be able to provide scheduled and on-demand scanning for mobile devices
163	Solution should have schedule update functionality for AV updates.
164	Solution should have functionality where update will start only if WiFi is available.
165	Solution should integrate advance threat protection data
166	Solution should have a (In/Out) filter for Calls and SMS with blacklist and White list feature
167	Solution should have a categorized Web URL and Application list with selective white listing and Block listing
168	Solution should be able to block network transactions for a particular specific application
169	Solution should have Anti-Theft functionality
170	Solution should have a location history function to keep the location data for any user
171	Solution should have a wipe function in case of the device is stolen
172	Solution should have a function to send alert to admin in case of a SIM change
173	Solution should be able to provide a type of password policy for both Android and IOS
174	Solution should have a Device control for USB/Camera/GPS .

175	Solution should be able to create application list which forms the allowed or compliant list and is allowed to function
176	Solution should have WiFi Control and able to connect to only defined SSIDs
177	Solution should send alarm or get locked if not connected to defined SSIDs lists
178	Solution should be able host a content library where data can be shared for collaborative work
179	Should be able to separate business and personal data. The business data should be encrypted. Should be able to follow BYOD and COD Policies. – Container
180	Solution should be inclusive of SIEM data collector
181	Solution should include geo fencing for devices
182	Solution should be able to show location history of the device
183	Solution should have content library for data sharing between groups - collaborative working
184	Solution should have its own App Store to share and deploy Organization software
185	Solution should have KIOS mode functionality
186	Solution should have a complete asset management inbuilt for Mobile Devices
187	Solution should be able to integrate with CRMs and SIEMS, SysLog Severs

B) Scope for Implementation of Active Directory		
A	**Hardware Configuration Setup**	
	1	Server Configuration for Windows 2016/2019/2022
	2	Operating System Installation (OS) Windows 2016/2019/2022(License will be provided by Bank)
	3	Configure Primary Domain controller
	4	Configure Primary DNS Configuration For DC,DR,HO and Branches
	5	To configure file server
B	1	Setup of internal domain to host the Active Directory. It is recommended to have a domain that is separate to the external domain.
	2	Dynamic Access Control
	3	Forest and domain structure
	4	Setup of the Organizational Units to be included in the Active Directory
	5	Setup of Users to be included in the Active Directory
	6	Setup of devices to be included in the Active Directory
	7	Setup of Group Policy
	8	Sharing of folders as per the requirement & Permission
	9	Setup of Password policy and password synchronization parameters
	10	Configure the Secondary DNS Server

	11	Configuration of file server roles
C	**User Profile Setup**	
	1	Create User Profile
	2	User Creation
	3	User Maintenance (Addition/Deletion/Disable/Enable)
	4	User Authentication
	5	User Rights
	6	Access Rights
	7	User Roaming Profile
	8	Link email ID to the User Profile if available
	9	Configure Minimum (Password) Length and Age of Passwords to meet banks Password Policy
	10	Setup of Primary and Secondary Servers to host the Active Directory - As per bank's policy and availability of infrastructure
	11	A/C Lockout Duration / Thresholds
	12	Map Users permission to files servers folder
D	**Synchronization**	
	1	Synchronization of the Primary Domain Controller and Secondary Domain Controller Servers if available to ensure auto failover & failback without disrupting service
E	**Desktop Configuration for Active Directory**	
	1	Take Backup of the Desktop if required in case of challenges
	2	Include the Desktop in the domain
	3	Include the Desktop in the Organizational Unit
	4	Restore the data on Desktop if required
F	**Essential Properties setup**	
	1	Flexible Single-Master Operation (FSMO) Compatibility to be checked
	2	Prohibit Access to properties of LAN connections
	3	Hide Settings Tabs
	4	Audit A/C Management
	5	Restrict CD ROM Access Local logged Users
	6	Remove Access to use all Windows updates
	7	Turn off Desktop Gadgets
	8	Restrict Un-Authorized S/W installation
	9	Disable local admin login
	10	Disable display of last login
	11	Configuring Windows Update Service
	12	Integration of Active Directory with End Point Protection Solution available with bank if any
	13	No auto Restart features

7. Commercial Bid format

The vendor, who is able to meet the specifications, features, scope mentioned in the above tables (A) and (B) should submit the bid in the following format:

S.N.	Particulars	Price	Remark if any
1.	(A) Endpoint Protection Solution with 50 licenses as per table (A) above with 3years Subscription, installation at all offices/branches of the bank etc.		
2	(B) Active Directory implementation for entire computer system of the bank, scope as per table (B) above.		
3	Taxation		

8. Payment terms

Payment **100%** will be done after the successful installation of the product solution at the branches, offices of the Bank and as per the requirement of the Bank.

---------- || ----------