The Kangra Central Cooperative Bank Ltd
Dharamshala H.P. 176 215

Tender Number KCCB/IT/CBS/2021/01

Document Cost Rs.1000/-

Last Date of Submission of Bid Documents :- 06/09/2021 upto 1.00 PM
Bid opening :- 06/09/2021, 3.00 PM

Tender For Supply and Installation of Enterprise Anti-Virus Software License

Tender for Supply and Installation of Enterprise Anti-Virus Software License

1. Introduction

The Kangra Central Co-Operative Bank Limited, Dharamshala is currently operating in five districts of Himachal Pradesh viz Kangra, Hamirpur, Una, Kullu and Lahaul & Spiti. The Bank has a network of 18 Zonal Offices, 216 Branches and 12 Extension Counters with it's Head Office at Dharamshala.
The Kangra Central Co-operative Bank Limited invites sealed tenders for the "Providing Licenses, Installation, Configuration, Deployment, Updating and Technical Support for Centralized Antivirus Server Solution with Endpoint Client Agent Deployment" from Original Equipment Manufactures (OEM)/ Service Provider/ Authorized Dealer or Distributor or Authorized Business Partner of OEM/Service Provider.
Bids should be sealed and superscribed with tender number and due date of submission and addressed to "**The Managing Director, The Kangra Central Co-operative Bank Ltd, Head Office Dharamshala (HP) – 176215**"

The sealed bids should reach at the address given above, latest by 06/09/2021 upto 1:00PM and it will be opened on 06/09/2021 at 3:00PM in the Conference Hall at Head Office of the Bank at Dharamshala.

2. Time schedule:

Tender Reference number	Tender Number KCCB/IT/CBS/2021/01 dated 19/08/2021.
Issue of Tender	21/08/2021 – 06/09/2021
Time and Last Date for receipts of bids	06/09/2021 upto 1:00 PM
Place of Opening tender offers	The Kangra Central Co-operative Bank Ltd, Head Office Dharamshala (HP) – 176215
Address of Communication	The Managing Director, The Kangra Central Co-operative Bank Ltd, Head Office Dharamshala (HP) – 176215
Contact Telephone Numbers	Phone: 01892–222269, Ext. 252, 301, 321 E mail : it@kccb.in

3. Cost Of The Tender Document

The Bidder shall deposit Rs. 1000/- (Rupees One Thousand Only) in the form of a Demand Draft favoring Managing Director, The Kangra Central Cooperative Bank Limited payable at Dharamshala being the cost of the tender document along with the Bid. Payment made through any other mode will not be accepted and decision of the Bank in this regard shall be final, conclusive and binding on the Bidder.

4. Earnest Money

Earnest Money @ Rs. 50,000/- (Rupees Fifty Thousand Only) should be submitted along with the Tender in the form of Demand Draft payable in favour of the Managing Director, The Kangra Central Cooperative Bank Limited at Dharamshala. Tenders without Earnest Money shall be out rightly rejected.

5. Bid Submission

The Technical and Commercial bids shall be submitted in separate sealed envelopes clearly super scribing on the envelope "Technical Bid for Supply and Installation of Enterprise Anti-Virus Software License as per Tender Number KCCB/IT/CBS/2021/01 dated 19/08/2021 " & " Commercial Bid for Supply and Installation of Enterprise Anti-Virus Software License as per Tender No Tender Number KCCB/IT/CBS/2021/01 dated 19/08/2021 " on or before 1:00 PM of 06/09/2021.

6. Bidders Eligibility Criteria

Bidders must meet the following eligibility requirements. Bids of non - compliant bidders will not be technically or financially evaluated.

1. The Bidder shall provide evidence that it is a current legal entity.
2. The Bidder/System Integrator should be the authorized representative /partner of the OEM. The proof in support of the same must be enclosed.
3. Should have experience in the following fields: Supply and Installation of Enterprise Anti-Virus / Endpoint Security Software License for government and financial organizations.
4. Bidder must warrant that key project personnel, should have minimum OEM certified engineers / equivalent certification / knowledge on Technology related to Antivirus and Endpoint Security Software, and should have been sufficiently involved in similar past installation.
5. Bidder must have back-to-back support relation with the OEM's whose products are offered by the bidder to the Bank. The proof in support of the same must be enclosed.
6. The last three financial years' audited Balance Sheet and Profit and Loss reports shall be provided.
7. The Bidder must demonstrate that it has been engaged in providing similar services for other large National /International Financial / Banking Institutions.
8. The Bidder shall provide references (including Referee names and contact details) in respect of major projects of similar type completed in the last five (3) years by the Bidder in any large organization and having its offices/branches across India.
9. The Bidder must warrant that there is no legal action being taken against it for any cause in any legal jurisdiction. If such an action exists and the Bidder considers that it does not affect its ability to deliver the Tender requirements, it shall provide details of the action(s).
10. Details regarding the fulfillment of the eligible criteria should be submitted as per Annexure – I.

4 Terms & Conditions:

1. All bids and supporting documentation shall be submitted in English.
2. All costs and charges, related to the bid, shall be expressed in Indian Rupees only and the above total cost is inclusive of installation charges and customization charges. The Kangra Central Co Operative Bank will not take into consideration, any variation in the $ price.
3. The Bank may opt to empanel more than one vendor, at L – 1 price of Para – 6 (b), if agreed upon by bidders.

4. **PERFORMANCE GUARANTEE:** EMD of successful Bidder will be retained as Performance Guarantee and will be returned after a period of six months after commissioning of the project and deduction of penalty if any. NO INTEREST would be payable on this amount.
5. Supply And Installation of Enterprise Anti-Virus Software License for Head Office Dharamshala, 18 Zonal Offices, 216 Branches and 12 Extension Counter should be completed within 08 (Eight) weeks from the date of purchase order.
6. License support is required for a period of three years as a comprehensive license support.
7. After the initial license period, the vendor has to provide the acceptance for extending license support for further 3 years, if required by the Bank, at mutually agreed rates.
8. The Kangra Central Co Operative Bank reserves the right to reject all or any of the quotations without assigning any reason thereof.
9. The bidder should work in close association with other vendors/service providers working for the Bank.
10. The decision of the Bank shall be final.

5 Earnest Money Deposit:

I. The Bidder shall furnish, as part of its bid, bid security of an amount equal to Rs. 50,000/- (Rupees Fifty Thousand Only). The bid security is required to protect the Bank against the risk of Bidder's conduct.
II. The bid security shall be denominated in the **INDIAN RUPEES** only and shall be in the form of a Demand Draft issued by an Indian Bank not earlier than the date of issue of this Tender, payable to **The Managing Director, The Kangra Central Cooperative Bank Limited at Dharamshala, H.P**. Any bid not secured in accordance with the above will be rejected as non-responsive.
III. Unsuccessful Bidder's bid security will be returned as promptly as possible but not later than 30 days after the expiration of the period of bid validity prescribed by the Bank.
IV. EMD of successful Bidder will be retained as Performance Guarantee and will be returned after a period of six months after commissioning of the project and deduction of penalty if any. NO INTEREST would be payable on this amount.
V. No claim shall lie against the KCCB in respect of erosion in the value or interest on the amount of earnest money deposit or security deposit.
VI. The bid security may be forfeited:
    - if a Bidder withdraws its bid during the period of bid validity; Or
    - if a Bidder makes any statement or encloses any form which turns out to be false, incorrect and / or misleading at any time and / or conceals or suppresses material information; Or
    - in case of the successful Bidder, if the Bidder fails to sign the agreement.

6 Bidding Process

A two stage bidding procedure will be followed. The response to the present tender should be submitted in two parts i.e. the Technical Bid and the Commercial Bid.

a. The Technical Bid:

The Technical and Commercial Specifications for Antivirus Software is enclosed as Annexure II

The bidders are required to submit a copy of the Technical Bid highlighting the features of proposed software. The Technical format and Specifications sheet enclosed as Annex I I to be submitted with compliance.

b. The Commercial Bid:

The bidders are required to submit a Commercial bid as per the Commercial Bid format enclosed as Annex III.

In the first stage, only the 'Technical Bids' of those who fulfill the eligibility criteria will be opened and evaluated. Those bidders satisfying the technical requirements of Annex – I, and II, as determined by the Bank and as per the requirements/specifications and the terms and conditions of this document, shall be short-listed.

In Second Stage, Commercial bids of technically qualified vendors will be opened. The commercial bids will be evaluated based on L1 criteria. The bidder who quote the lowest price shall be considered as L1.

The Bidder must organize the bid in accordance with the format specified in the tender document.

The Bidder is liable to be rejected if any commercial details are found along with the technical bid.

c. List of Annexures:

Sno	Formats	Description
1	Annexure - I	Bidder Eligibility Criteria
2	Annexure - II	Technical Specification for Anti-Virus Solution
3	Annexure - III	Commercial Bid of Antivirus Software Solution for 3 Years
4	Annexure – IV	Manufacturer's Authorisation Form (MAF)
5	Form "A"	Technical Deviation Statement

7 Objective of the project

The primary objective of this tender is to have Endpoint Protection Solution with Online Monitoring Solution.

The proposed solution should be agnostic to the underlying hardware, storage, network, operating system, and Hypervisors. In addition, it should integrate with the existing infrastructure management setup currently deployed at the Bank.

8 Technical and Solution requirement Specifications

Overview

The bidder is required to propose the Total Solution supporting features/functionality as indicated in **Annexures.**
The Total Solution shall be hosted at The Kangra Central Co Operative Bank, Dharamshala.

9 Scope of Work

The minimum specified scope of work to be undertaken by the selected bidder is mentioned below:

1. The "Total solution" will include Supply and Installation of Enterprise Anti-Virus Software License on the infrastructure mentioned below:

Sl No	Description	Number of Devices (Approx)
	a) Windows XP SP3 32-bit Edition b) Windows XPSP3 64-bit Edition	1200

1	c) Windows 7 d) Windows 8 e) Windows8.1 f) Windows10 and all future Windows desktop Operating System, 32-bit version & 64-bit version	
Exact number of installations may vary slightly. Payment will be made based on actual installations.		

2. Supply of Antivirus software as per technical specification mentioned in Annexures II, III and IV of the Tender.

3. Installation, integration of Antivirus software with Bank (Head Office Dharamshala, 18 Zonal Offices, 216 Branches and 12 Extension Counter).

4. The proposed solution should have provision of handshake / interface / integration with Bank's existing hardware and software at all levels.

5. The bidder should fix all the technical problems, provide and implement upgrades, updates free of cost to the Bank, as and when released by the OEM during license period.

6. The bidder shall address statutory requirements, network and security audit recommendations suggested by the Bank from time to time on regular basis without additional cost to the Bank.

7. The bidder to have back-to-back arrangement with OEM/Service provider for Support, updates and upgrades. Certificate for the same to be provided along with Technical bid. A Letter for support from original equipment manufacturer (OEM)/Service Provider shall also be submitted in addition to Manufacturer's Authorization Form for the contract period.

8. The Bank shall promptly notify the bidder in writing of any claims arising under this license. Upon receipt of such notice, the bidder shall with all reasonable speed, repair or replace the defective products or part thereof without cost to the Bank.

9. Software maintenance, and Support:

   a) The bidder shall provide free maintenance services during the period of years. During license period, the bidder shall provide upgrades, updates, patches and regular virus signature updates, etc. without any additional cost. During the contract period, the bidder must depute qualified maintenance engineer whenever required.

   b) The bidder shall ensure that faults and failures intimated by the Bank as above are set right within 24 hours of being informed of the same.

10 Training

A Comprehensive training shall be the key to successful Operations and Maintenance; hence, the Bidder is required to provide required training to the Bank nominated Officials at The Kangra Central Co Operative Bank Ltd, Dharamshala. The training documents, including Operating Manuals, Standard Operating Procedures (SOP) for the proposed solution shall be prepared and shared by the bidder with the Bank. The successful Bidder is free to propose the training plan. However, at a minimum, the plan shall include the following:

Sr No	Training Description
1	Overview of the components Installed
2	Technical Architecture

3	Operating procedure for Antivirus software
4	Installation procedure for Antivirus client and server license on varied Operating Systems
5	Technical and Operational Manual of the solution
6	Handling worst case scenarios (Malwares, Zero Day Vulnerabilities among others)

The above plan is only indicative; the final training plan shall be finalized between the successful bidder and the Bank.

No separate charges will be paid for training.User Acceptance Test

The implementation shall be deemed as completed in all respects only after:

a. Implementation is done as per the intent of this tender;
b. Enabling all the functionalities mentioned therein, i.e., go-live; and
c. All the related trainings are completed
d. The Bidder is expected to state the implementation plan and methodology and Bank's team and the bidder shall jointly decide the roll out methodology.

11 Period of Validity

All the prices and other terms and conditions of the offer proposed by the Bidder should be **Valid** for a **minimum** period of ***Three months***.

12 Correction of Errors

Arithmetic errors in bids will be treated as follows:

Where there is a discrepancy between the amounts in figures and in words, the amount in words shall govern.
Where there is a discrepancy between the unit rate and the line item total resulting from multiplying the unit rate by the quantity, the unit rate will govern unless, in the opinion of the Bank, there is obviously a gross error such as misplacement of a decimal point, in which case the line item total will govern.

Where there is a discrepancy between the amount mentioned in the bid and the line item total present in the Bill of Material, the amount obtained on totaling the line items in the Bill of Materials will govern.

The amount stated in the tender form, adjusted in accordance with the above procedure, shall be considered as binding, unless it causes the overall tender price to rise, in which case the bid price shall govern.

13 Confidentiality

Bidder agrees that all mails, data, financial, mail architecture and personnel data relating to Bank's business and other information identified as confidential by the Bank, the same shall be kept confidential and shall not be shared with any third party without prior written approval from Bank.

14 Right to Verification

The Bank reserves the right to verify any or all statements made by the Bidder in the tender document and to inspect the Bidder's facility, if necessary, to establish to its satisfaction about the Bidder's capacity to perform the job.

15 Delivery & Installation Period

The following time schedule for completion of the activities from the date of placement of orders should be strictly adhered to. Delay in delivery and installation may invite penalties for the vendors.

a)	Delivery	≤ 4 Weeks
b)	Installation and Operationalization	≤ 4 Weeks

16 Payment Terms:

1. 100% payment will be made to the bidder on delivery, successful installation demonstration and training of the software product.

17 Obligations of Successful Bidder

a. The successful bidder has to supply all the components, services and licenses to make solution complete.

b. The successful bidder shall deploy their own trained and experienced engineers for implementing, managing and maintaining the system.

c. Whenever any new threats / vulnerabilities become public, the bidder/successful bidder shall bring this to the notice of Bank immediately and help/guide Bank in plugging the same. Once the call has been attended, successful bidder engineers shall put their maximum efforts and deploy their best resources to resolve all calls at the earliest possible time frame at all locations and ensure appropriate uptime.

d. The bidder/successful bidder to ensure that during implementation of complete, the critical services hosted at the Bank shall not face any downtime due to security breach, security incident, improper configuration of security units/ appliances/ components.

18 Order Cancellation:

Bank reserves its right to cancel the order in the event of delay in delivery and installation beyond the stipulated time.

19 Penalty for Delay:

For any delay in installation and commissioning of the software solution beyond the specific period, Bank will charge penalty @ 0.5% of the order per week or part thereof, subject to a maximum of 5%. In case, the amount equals to 5% of the order value and is deductible as penalty and the bidder is still unable to complete successful Installation, the Bank reserves the right to cancel the order and no payment will be made to the bidder.

20 Penalty for Undetected Virus/Infection/Malware

The successful service provider must gurantee fixes to virus infections within maximum 2 hours after being made aware of the virus. Failure to provide fixes within 2 hours will result in an extension on current license period by one week.

21 Resolution of Disputes

Bank and the bidder shall make every effort to resolve amicably, by direct informal negotiation, any disagreement or dispute arising between them under or in connection with the contract. If after thirty days from the commencement of such informal negotiations, Bank and the bidder have been unable to resolve amicably a contract dispute, either party may require that the dispute be referred for resolution by formal arbitration.

22 Indemnification

1. The bidder/ successful bidder at its own cost and expenses defend and indemnify the Bank against all third-party claims including those of the infringement of Intellectual Property Rights, including patent, trademark, copyright, trade secret or industrial design rights, arising from use of the Products or any part thereof in India.

2. The bidder shall expeditiously meet any such claims and shall have full rights to defend itself there from. If the Bank is required to pay compensation to a third party resulting from such infringement, the bidder shall be fully responsible therefore, including all expenses and court and legal fees.

3. The Bank will give notice to the Bidder of any such claim and shall provide reasonable assistance to the bidder disposing of the claim.

4. The bidder shall also be liable to indemnify the Bank, at its own cost and expenses, against all losses/damages, which the Bank may suffer on account of violation by the bidder/successful bidder of any or all national/international trade laws, norms, standards, procedures, etc.

23 Liquidated Damages

The liquidated damages is an estimate of the loss or damage that the Bank may have suffered due to delay in performance or non-performance of any or all the obligations (under the terms and conditions of the purchase contract relating to supply, delivery, installation, operationalisation, implementation, training, support/services, acceptance, maintenance, etc., by the bidder/successful bidder and the bidder/successful bidder

shall be liable to pay the Institute a fixed amount for each day of delay / non-performance of the obligations by way of liquidated damages, details of which will be specified in the Tender. Without any prejudice to the Bank's other rights under the law, the Institute shall recover the liquidated damages, if any, accruing to the Bank, as above, from any amount payable to the Bidder either as per the tender, executed between the parties or under any other purchase agreement / contract, the Bank may have executed / shall be executing with the bidder/successful bidder.

24 Force Majeure

The bidder/successful bidder or the Bank shall not be responsible for delays or non-performance of any or all contractual obligations, caused by war, revolution, insurrection, civil commotion, riots, mobilizations, strikes, blockade, acts of God, Plague or other epidemics, fire, flood, obstructions of navigation by ice of Port of dispatch, acts of government or public enemy or any other event beyond the control of either party, which directly, materially and adversely affect the performance of any or all such contractual obligations.

If a Force Majeure situation arises, the bidder/successful bidder shall promptly notify the Bank in writing of such conditions and any change thereof. Unless otherwise directed by the Organization in writing, the bidder/successful bidder shall continue to perform his obligations under the contract as far as possible, and shall seek all means for performance of all other obligations, not prevented by the Force Majeure event.

25 Jurisdiction

The jurisdiction of the courts shall be Dharamshala, Himachal Pradesh.

For any questions/clarifications related to requirements, please contact us at it@kccb.in

Annexure I

Sno	Bidders Eligibility Criteria	Compliance Y/N	Supporting Documents enclosed Y/N
1	The Bidder shall provide evidence that it is a current legal entity.		
2	The Bidder/System Integrator should be the authorized representative/ partner of the OEM. The proof in support of the same must be enclosed.		
3	Should have experience in the following fields: Supply and Installation of Enterprise Anti-Virus / Endpoint Security Software License for government and financial organizations.		
4	Bidder must warrant that key project personnel, should have minimum OEM certified engineers / equivalent certification / knowledge on Technology related to Antivirus and Endpoint Security Software, and should have been sufficiently involved in similar past installation.		
5	Bidder must have back-to-back support relation with the OEM's whose products are offered by the bidder to Bank. The proof in support of the same must be enclosed.		
6	The last three financial years' audited Balance Sheet and Profit and Loss reports shall be provided.		
7	The Bidder must demonstrate that it has been engaged in providing similar services for other large National /International Financial / Banking Institutions.		
8	The Bidder shall provide references (including Referee names and contact details) in respect of major projects of similar type completed in the last five (5) years by the Bidder in any large organization and having its offices /branches across India.		
9	The Bidder must warrant that there is no legal action being taken against it for any cause in any legal jurisdiction. If such an action exists and the Bidder considers that it does not affect its ability to deliver the tender requirements, it shall provide details of the action(s).		
10	The cost of bidding and submission of tender documents is entirely the responsibility of bidders, regardless of the conduct or outcome of the tendering process.		

Annexure – II

Technical Specification for Anti-Virus Solution

Sl No	Required Specifications	Compliance (Yes/No), Comments (If any)
1	The Solution should provide multi-layer of protection into a single agent - (AV, NIPS, HIPS, Memory Exploit Mitigation, Advance Machine Learning, Emulation capabilities, Behavioural Monitoring and protection, reputation lookup, application and device control & system lockdown)	
2	Network threat protection should analyse incoming data and blocks threats while they travel through the network before hitting the system. Rules-based firewall and browser protection should be included to protect against web-based attacks.	
3	Signature-based antivirus should eradicate malware on a system to protect against viruses, worms, Trojans, spyware, bots, adware, and rootkits and also should offer comprehensive client/server security by protecting enterprise networks from viruses, Trojans, worms, hackers, and network viruses, plus spyware and mixed threat attacks.	
4	Correlate different linkages between users, files, and websites to detect rapidly mutating threats. By analysing key file attributes, The solution should accurately identify whether a file is good and assign a reputation score to each file, effectively protecting against targeted attacks.	
5	Have artificial intelligence to provide zero-day protection and stop new and unknown threats by monitoring file behaviours while they execute in real-time to determine file risk. Must be able to reduce the risk of virus/malware entering the network by blocking files with real-time compressed executable files.	
6	Remediation and side effect repair engine should aggressively scans infected endpoints to locate Advanced Persistent Threats and remove tenacious malware. Administrator should remotely be able to trigger this and remedy the infection remotely from the management console.	
7	The Solution should check for the existence for antivirus software, patches, hot fixes, and other security requirements. For example, the policy may check whether the latest patches have been applied to the operating system.	
8	The solution should enhance protection for business critical systems by only allowing whitelisted applications (known to be good) to run or by blocking blacklisted applications (known to be bad) from running. Finger printing of all applications should from centralized console.	
9	The solution should help prevent internal and external security breaches by monitoring application behaviour and controlling file access, registry access, processes that are allowed to run, and devices information can be written to.	
10	The solution should allow administrator to run custom scripts on their endpoints to verify and report compliance; quarantine location and peer-to-peer enforcement lockdown and isolate a non-compliant or infected system.	

11	The solution should automatically detects what location a system is connecting from, such as a hotspot, wireless network, or VPN and adjusts the security to offer the best protection for the environment.	
12	To address the threats and nuisances posed by Trojans, the solution should be able to do the following: Terminating all known virus processes and threads in memory, repairing the registry, Deleting any drop files created by viruses, removing any Microsoft Windows services created by viruses, restoring all files damaged by viruses, Includes Clean-up for Spyware, Adware etc	
13	The solution should automatically engage in an aggressive scan mode if it detects large number of malware or high-risk threats on windows clients.	
14	The solution should auto-compile, auto-protect when the operating system kernel is not compatible with precompiled auto-protect kernel module especially for Linux variants.	
15	If any endpoint is having more than three days older virus definition and if such endpoint tries to connect the network, then the solution must immediately install latest virus definition by connecting to the endpoint management server and blocking all connections to the other network resources like internet, intranet applications etc	
16	If the host is non-compliant with the policies, the solution must automatically initiate remedial action, which may include running isolating it from network, downloading and executing/inserting a software, running scripts, by setting required registries keys. The solution should recheck host for compliance after remediation and grant access for the compliant host to the network.	
17	The solution must be able check whether required software, security patches and hot fixes have not been installed on the endpoint as mandated by organization, the solution should be set to connect to an update server to download and install the required software based on the policy.	
18	The solution must have reports that incorporate multi-dimensional analysis and robust graphical reporting in an easy-to-use dashboard.	
19	The solution must have group update provider reduces network overhead and decreases the time it takes to get updates by enabling one client to send updates to another, enabling more effective updates in remote locations.	
20	Must provide Real-time lock down of client configuration – allow or prevent users from changing settings or unloading/uninstalling the software	
21	Users with the scheduled scan privileges can postpone, skip, and stop Scheduled Scan.	
22	Solution should detect command and control traffic activity with IP level events, URL events, and DNS activity using detection mechanisms like static analysis, behavioural analysis, and reputation analysis from intelligence network.	
23	CPU usage performance control during scanning: 1) Checks the CPU usage level configured on the Web console and the actual CPU consumption on the computer 2) Adjusts the scanning speed if: The CPU usage level is Medium or Low and Actual CPU consumption exceeds a certain threshold	
24	Safeguards endpoint mail boxes by scanning incoming POP3 email and Outlook folders for Threats	

25	Solution should have dashboard to include the latest high risk tasks, search capabilities, recent samples, multiple processing stats, e.g. event count, tasks complete, and risk scores over say last 24 hours	
26	Should be able to deploy the Client software using the following mechanisms: 1)Client Packager (Executable & Microsoft Installer (MSI) Package Format), 2)Web install page, 3)Login Script Setup, 4)Remote installation, 5)From a client disk image	
27	The solution should manage single license for windows, Linux and mac Operating Systems and management server should not be separate.	
28	The solution should detect malware that evades detection by using polymorphic custom packers by unpacking in a lightweight virtual environment with no performance over-head.	
29	Must provide a secure Web-based management console to give administrators transparent access to all clients and servers on the network	
30	Solution should provide anomaly detection to detect and report on suspicious information found in a file. Preferable capabilities should include, TLS call-back activity, CVE and exploit detection, shell-code detection, debugger detection, watermark tampering, and non-standard file alignment, RFC compliant etc	
31	The solution should set up peer-to-peer authentication policy, which can grant or block inbound access to the remote computers that have the client installed.	
32	The Solution should provide manage windows, Linux and mac agents from same centralized console.	
33	The solution should download content updates from the central server when computers are idle so that it does not affect bandwidth. Must reduce network traffic generated when downloading the latest pattern by downloading only incremental patterns	
34	If the endpoint client detects a network attack, solution must automatically activate active response to block all communication to and from the attacking computer	
35	Should have role based administration with active directory integration: To create custom role type, To add uses to a predefined role or to a custom role. Shall support grouping of clients into domains for easier administration	
36	The Solution must have a layer of protection that enables organization to go on the offensive, lure attackers out of hiding, and reveal attacker intent and tactics via early visibility, so that the information can be used to enhance security posture.	
37	The solutions should be able expose advanced attacks with precision machine learning, behavioural analytics and threat intelligence minimizing false positives.	
38	The Solution should provide report over email, CSV, html or pdf.	
39	The solution should be in the leader’s quadrant of latest Gartner Report for endpoint security.	
40	The solution 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 capabilities to clients and servers across the network	
41	The solution should 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 capabilities to clients and servers across the network.	

42	The solution should allow definition update to be done manually on management servers. Either by using a machine where internet is available or from there you can copy the files to offline management servers.	
43	The solution Should help prevent internal and external security breaches by monitoring application behaviour and controlling file access, registry access, processes that are allowed to run, and devices information can be written to	
44	The Solution should able to block devices based on Windows Class ID and should include USB, Infrared, Bluetooth, Serial, Parallel, fire wire, SCSI and PCMCIA. Solution should also be able to block and give read/write/execute permission for mentioned devices	

Annexure – III

Commercial Bid

Commercial Bid of Antivirus Software Solution for 3 Years (Amount in ₹)

Sno	Description	Client License Qty	Unit Price	Taxes in %	Taxes *f=d*e*	Total Amount *g=c*(d+f)*
		c	d	e	f	g
1	Antivirus / Endpoint Solution					
	Grand Total in Rs					

Annexure IV

MANUFACTURER'S AUTHORISATION FORM (MAF)

No._____Dated _____

To

We _____ who are established and reputable providers of _____ having offices at _____and _____do hereby authorize

M/s_____(Name and address of Agent /Dealer) to offer their quotation, negotiate and conclude the contract with you against the above invitation for tender offer.

We hereby extend our full guarantee and warranty as per the terms and conditions of the tender and the contract for the services offered against this invitation for tender offer by the above firm.

Yours faithfully,

(Name) for and on behalf of M/s_____
(Name of Provider)

Note: This letter of authority should be on the letterhead of the service provider concerned and should be signed by a competent authority of the service provider.

Form "A"

Technical Deviation Statement

The following are the particulars of deviations from the requirements of the bidder specifications:

Sno	Clause	Annexure No	Deviation	REMARKS (Including justifications)

The technical specifications furnished in the bidding document shall prevail over those of any others document forming a part of our bid except only to the extent of deviations furnished in this statement.

Dated .....

Signature and seal of the Bidder

Note: Where there is no deviation, the statement should be returned duly signed with an endorsement indicating "No Deviations".