



KERALA INSTITUTE OF LOCAL ADMINISTRATION (KILA)

MULAMKUNNATHUKAVU P.O., THRISSUR-680 581

T E N D E R

Containing General conditions of contract for the **Supply,Installation and Commissioning of Endpoint Protection Solution with 3 Year License for 120 Client Devices .**

Issued to :

Issued on :

Last date and time for the receipt of tender : **15-11-2017. 3 PM**

(To be filled in by the Tenderer)

Name and Address of tenderer (in full) :

EMD amount :

DD No. and date :

Submitted on :

Signature of Tenderer

Document 2017/101/12083 - GENERAL - File No. 2017/101/3339
Approved by Director on 02/11/2017 20:50:10

<http://www.kila.ac.in>
UcwbLB-NrH-ocFH-di.mzN



KILA, Mulamkunnathukavu Thrissur



Document 2017/101/12083 - GENERAL - File No. 2017/101/3339
Approved by Director on 02/11/2017 20:50:10

<http://www.kila.ac.in>
UcwbhB-NrH-ocfH-di.mzN



KILA Mulankunathukavu, Thrissur

K.F.C. FORM 14
(See Chapter VII, Article 143)

FORM OF TENDER

Sir,

I/We hereby tender to supply, under the annexed general and special conditions of contract, the whole of the articles referred to and described in the attached specification and schedule, or any portion thereof as may be decided by KILA at the rates quoted against each item. The articles will be delivered within the time and at the places specified in the schedule.

I/we/am/are remitting/have separately remitted the required amount of Rs..... as earnest money.

Yours faithfully,

(Signature)

(Address)

.....

Date

To be scored in case where no earnest money deposits is furnished.



GENERAL CONDITIONS

Sealed tenders are invited for the supply, Installation and Commissioning of Endpoint Protection Solution with three Year License for 120 Client Devices at KILA, Mulamkunnathukavu

General Conditions:

1. The tenders should be addressed to the Director, Kerala Institute of Local Administration, Mulamkunnathukavu, Thrissur, Pin-680581 in a sealed cover with the tender number and name as mentioned in the special condition shown below duly superscribed on the cover.
2. The tenders should be in the prescribed form which can be obtained from the officer mentioned below on payment of the price which is also noted below. Duplicate copies of tender forms will also be issued at the rate specified below. The cost of tender forms once paid will not be refunded. Tenders which are not in the prescribed form are liable to be rejected. The rates quoted should be only in Indian currency. Tenders in any other currency are liable to rejection.
3. Intending tenderers should send their tender so as to reach the officer mentioned below, on due date and time (noted below). No tender received after the specified date and time will be accepted on any account. The rates will be considered firm for acceptance till the tenders are processed. Tenders with price variation clause and/or 'subject to prior sale' conditions are liable to be rejected.
4. (a) Every tenderer who has not registered his name with the State Government (Stores Purchase Department) should send along with his tender, an earnest money of one per cent of the total cost of the articles tendered for (rounded to the nearest rupee) subject to a minimum of Rs. 30, if the amount calculated at one per cent of the value of the articles tendered for falls below Rs. 30. The amount may be paid by demand drafts (crossed) drawn in favour of Director, KILA, Thrissur payable at Thrissur. Cheques will not be accepted. The earnest money of the unsuccessful tenderers will be returned as soon as possible after the tenders are settled; but that of the successful tenderers will be adjusted towards the security that will have to be deposited for the satisfactory fulfillment of the contract. No interest will be paid for the earnest money deposited.
(b) Tenderers whose names are registered with Government (Store Purchase Department) are generally exempted from furnishing earnest money for such articles or which they have registered their names. If they tender for stores other than those for which they have registered their names they will have to furnish earnest money as in the case of unregistered firms. Registered firms will have to quote invariably in every tender they submit the registration number assigned to them by the Stores Purchase Department.
(c) (i) Small Scale Industries and Cottage Industries and Industrial Co-operative within the State which are certified as such by the Director of Industries and Commerce or by the Regional Joint Directors of Industries and Commerce will be exempted from furnishing earnest money deposits in support of tenders submitted by them to Government Departments. The Khadi and Village Industries Co-operative Societies and the institutions registered under the literary, Scientific and Charitable Societies Act and financed by the Kerala Khadi and Village Industries Board within the State which are certified as such by the Secretary, Kerala Khadi and Village Industries



Board will be exempted from furnishing earnest money deposits in support of tenders.

(ii) Small Scale Industries, Cottage Industries and Industrial Co-operatives within the State which have been registered as such with the Industries Department (Department under the control of the Director of Industries and Commerce) on furnishing proof of such registration will be exempted from furnishing security deposits against contracts for supply of stores manufactured by them provided that an officer of and above the rank of Deputy Director of Industries and Commerce having jurisdiction over the area also certifies to the soundness, and reliability of the concerns to undertake the contracts. The Khadi and Village Industries Co-operative Societies within the State which have been registered as such with the Kerala Khadi and Village Industries Board and the Institutions registered under the Literary, Scientific and Charitable Societies Act and which are financed by the Board within the State on furnishing proof of such registration will be exempted from furnishing security deposits against contracts for supply of stores manufactured by them provided that the Secretary, Kerala Khadi and Village Industries Board also certifies to the soundness and reliability of the concerns to undertake the contracts.

(d) In the matter of purchase of stores Small Scale Industrial Units sponsored by the national Small Industries Corporation Ltd. New Delhi and in respect of which competency certificates are issued by the Corporation will be exempted from payment of earnest money deposits and security deposits.

(e) The exemption stipulated in clause (b) and (c) above will not however, apply to tenders for the supply of raw Materials, or dietary articles or supply of stores on rate or running contract basis.

5. The tenders will be opened on the appointed day and time in the office of the undersigned, in the presence of such of those tenderers or their nominees who may be present at that time.

6. If any tenderer withdraws from his tender before the expiry of the period fixed for keeping the rates firm for acceptance, the earnest money, if any, deposited by him will be forfeited or such action taken against him as think fit. Tenderers shall invariably specify in their tenders the delivery conditions including the time required for the supply of articles tendered for.

(a) The tenderer shall clearly specify whether the articles offered bear Indian Standards Institution Certification Mark or not. In such cases, they shall produce copies of certification mark along with their tender in support of it.

(b) Tenderers shall clearly specify whether the goods are offered from indigenous sources, from imported stocks in India or from foreign sources to be imported under a license. KILA reserve the right to reject offers for import of goods if the import trade control policy in force at the time of award of the contract prohibits or restricts such imports.

7. The final acceptance of the tender rests entirely with the KILA who do not bind themselves to accept the lowest or any tender. But the tenderers on their part should be prepared to carry out such portion of the supplies included in their tenders as may be allotted to them.

8. In the case of materials of technical nature the successful tenderer should be prepared to guarantee satisfactory performance for a definite period under a definite penalty.

9. Communication of acceptance of the tender normally constitutes a concluded contract. Nevertheless, the successful tenderer shall also execute an agreement for the due fulfillment of the contract within the period to be specified in the letter of acceptance.



10. The contractor shall have to pay all stamp duty, lawyer's charges and other expenses incidental to the execution of the agreement. Failure to execute the agreement within the period specified will entail the penalties set out in para 12 below.

(a) The successful tenderer shall, before signing the agreement and within the period specified in the letter of acceptance of his tender, deposit a sum equivalent to 5 per cent of the value of the contract as security for the satisfactory fulfillment of the contract less the amount of money deposited by him along with his tender. The amount of security may be deposited in the manner prescribed in clause 4 supra. Letters of guarantee in the prescribed form for the amount of security from an approved Bank will also be considered enough at the discretion of KILA. If the successful tenderer fails to deposit the security and execute the agreement as stated above, the earnest money deposited by him will be forfeited to KILA, and the contract arranged elsewhere at the defaulter's risk and any loss incurred by KILA on account of the purchase will be recovered from the defaulter who will, however, not be entitled to any gain accruing thereby. If the defaulting firm is a registered firm their registration is liable to be cancelled.

(b) In case where a successful tenderer, after having made partial supplies fails to fulfil the contracts in full, all or any of the materials not supplied may at the discretion of the Purchasing Officer, be purchased by means of another tender/quotation or by negotiation or from the next higher tenderer who had offered to supply already and the loss, if any, caused to the KILA shall thereby together with such sums as may be fixed by the Director, KILA towards damages be recovered from the defaulting tenderer.

(c) Even in cases where no alternate purchase are arranged for the materials not supplied, the proportionate portion of the security deposit based on the cost of the materials not supplied at the rate shown in the tender of the defaulter shall be forfeited and balance alone shall be refunded.

11. The security deposit shall subject to the conditions specified herein, be returned to the contractor within three months after the expiration of the contract, but in the event of any dispute arising between the KILA and the contractor the Director, shall be entitled to deduct out of the deposits or the balance thereof, until such dispute is determined, the amount of such damages, costs, charges and expenses as may be claimed. The same may also be deducted from any other sum which may be due at any time from KILA to the contractor. In all cases where there are guarantee/warranty for the goods supplied the security deposit will be released only after the expiry of the guarantee/warranty period and subject to the special condition No.10.

12. (a) All payments to the contractors will be made by the Director in due course by cheques or drafts through Bank or District Treasury, Thrissur.

(b) All incidental expenses incurred by the KILA for making payments outside the District in which the claim arises shall be borne by the contractor.

13. The tenderers shall quote also the percentage of rebate (discount) offered by them in case the payment is made promptly within fifteen days/within one month of taking delivery of stores.

14. The Contractor shall not assign or make over the contract or the benefits or burdens thereof to any other person or body corporate. The contractor shall not underlet or sublet to any person or persons or body to corporate the execution of the contract or any part thereof without the consent in writing of the Purchasing Officer who shall have absolute power to refuse such consent or to rescind such consent (if given) at any time if



allowance or compensation shall be made to the contractor or the sub-contractor upon such rescission. Provided always that if such consent be given at any time, the contractor shall not be relieved from any obligation, duty or responsibility under this contract.

- 15.(a) IN case the contractor becomes insolvent, or goes into liquidation, or makes or proposes to make any assignment for the benefit of his creditors or proposes any composition with his creditors, for the settlement of his debts, carries on his business or the contract under inspection on behalf of his creditors, or in case any receiving order or orders for the administration of his estate are made against him or in case in which under any clause or clauses of this contract the contractor shall have rendered himself liable to damages amounting to the whole of his security deposits, the contract shall, thereupon after notice given by the Director to the Contractor be determined and the Director, KILA may complete the contract in such time and manner and by such persons as the Director shall think fit. But such determination of the contract shall be without any prejudice to any right or remedy of the KILA against the contractor or his sureties in respect of any breach of contract therefore committed by the contractor. All expenses and damages caused to by any breach of contract by the contractor shall be paid by the contractor to KILA and may be recovered from him under the provisions of the Revenue Recovery Act in force in the State.

(b) The persons/contractors submitting tenders should produce a solvency certificate, clearly indicating to what extent they are solvent from the Tahsildar of the Taluk where they reside, along with their tenders.

Note:- The solvency certificate referred to above will apply only in the case of supply of the following articles, viz., dietary articles, fuels, raw materials like roots, creepers, flowers etc., and provisions to hospitals and hostels sundry articles, etc.

- 16.(a) In case the contractor fails to supply and deliver any of the said articles and things, within the time provided for delivery of the same, or in case the contractor commits any breach of any of the covenants stipulations and agreements herein contained, and in his part to be observed and performed, then and in any such case, it shall be lawful for Director (if they shall think fit to do so) to arrange for the purchase of the said articles and things from elsewhere or on behalf of the KILA by an order in writing under the hand of the Purchasing Officer put an end to this contract and in case the KILA shall have incurred, sustained or been put to any costs, damages or expenses by reason of such purchase or by reason of this contract having been so put and end to or in case any difference in price, compensation, loss, costs, damages, expenses or other moneys shall then or any time during the continuance of this contract be payable by the contractor to the KILA under and by virtue of this contract, it shall be lawful for the KILA from and out of any moneys for the time being payable or owing to the contractor from the KILA under or by virtue of this contract or otherwise, to pay and reimburse to the KILA all such costs, damages and expenses they may have sustained, incurred or been put to by reason of the purchase made elsewhere or by reason of this contract having been so put an end to as aforesaid and also all such difference in price, compensation, loss costs, damages, expenses and other money's as shall for the time being the payable by the contractor aforesaid.

(b) In case any difference or dispute arises in connection with the contract, all legal proceedings relating to the matter shall be instituted in the Court within whose jurisdiction the Director, KILA voluntarily resides.

- 17..Any sum of money due and payable to the contractor (including security deposit returnable to him) under this contract may be appropriated by the purchasing officer or



any other person authorised by KILA and set off against any claim of the Purchasing Officer, KILA for the payment of a sum of money arising out of or under any other contract made by the contractor with KILA or any other person authorised by Director, KILA. Any sum of money due and payable to the successful tenderer or contractor from KILA shall be adjusted against any sum of money due to KILA from him under any other contracts.

18. Every notice hereby required or authorised to be given may be either given to the contractor personally or left at his residence or last known place of abode or business, or may be handed over to his agent personally, or may be addressed to the contractor by post at his usual or last known place of abode or business and if so addressed and posted shall be deemed to have been served on the contractor on the date on which, in the ordinary course of post, a letter so addressed and posted would reach his place of abode or business.
19. The tenderer shall undertake to supply materials according to the standard sample and/or specifications.
20. No representation for enhancement of rates once accepted will be considered.
21. Any attempt on the part of the tenderers or their agents to influence the Director, KILA in their favour by personal canvassing with the Officers concerned will disqualify the tenderers.
22. Tenderers should be prepared to accept orders subject to the penalty clause for forfeiture of security in the event of default in supplies or failure to supply within the stipulated period.
23. Telegraphic quotations will not be considered unless they give details of prices and are immediately followed by confirmation with full relevant details posted before the due date of the tender.
24. The prices quoted should be inclusive of all taxes, duties, cesses, etc., which are or may become payable by the contractor under existing or future law or rules of the country of origin supply or delivery during the course of execution of the contract.
25. The tenderer will invariably furnish the following certificate along with their bills for payment:-
"Certified that the Goods on which GST has been charged have not been exempted under the GST Act or the Rules made thereunder and the charges on account of GST on these goods are correct under the provisions of the relevant Act or the rules made thereunder. Certified further that we (or our Branch or Agent).
(Address)

are registered as dealers in the State of under
Registration, No..... for purposes of GST".

(Authorised signature with seal)

26. Special conditions, if any, of the tenderers attached with the tender will not be applicable to the contract with the tender unless they are expressly accepted in writing by the purchaser.
27. The tenderer should send along with his tender an agreement executed and signed in Kerala stamp paper of value Rs.200 purchased in the Kerala State. A specimen form of agreement is given as annexure to this tender. Tenders without the agreement in



Document 2017/101/12083 - GENERAL - File No. 2017/101/3339
Approved by Director on 02/11/2017 20:50:10

<http://www.kila.ac.in>
UcwhB-NrH-ocFH-di.mzN



KILA, Mulankunathukavu, Thrissur

not been received, the Purchasing Officer may exercise his discretion and call upon such tenderer to execute the agreement within a period of ten days from the date of issue of such intimation, if the Purchasing Officer is satisfied that the omission to forward the agreement along with the tender was due to causes beyond the control of the tenderer and was not due to any negligence on his part. Agreement received from a tenderer after the above time limit will not be considered.



ANNEXURE

Agreement

Articles of Agreement executed on this the day oftwo thousand Between the Director, KILA (hereinafter referred to as the Director of the one part and Shri..... (H.E. name and address of the tenderer) (hereinafter referred to as "the bounden") of the other part.

Whereas in response to the notification No.dated the bounden has submitted to the Director a tender for the specified therein subject to the terms and conditions contained in the said tender;

Whereas the bounden has also deposited with the Director a sum of Rs. as earnest money for execution of an agreement undertaking the due fulfillment of the contract I case his tender is accepted by the Managing Director.

Now these presents witness and it is hereby mutually agreed as follows:-

1. In case the tender submitted by the bounden is accepted by the Director and the Contract for is awarded to the bounden, the bounden shall within days of acceptance of his tender execute an agreement with the Director incorporating all the terms and conditions under which the Director accepts his tender.

2. In case the bounden fails to execute the agreement as aforesaid incorporating the terms and conditions governing the contract the Director shall have power and authority to recover from the bounden any loss damage caused to the KILA by such breach as may be determined by the Director by appropriating the earnest money deposited by the bounden and if the earnest money is found to be inadequate the deficit amount may be recovered from the bounden and his properties movable and immovable in the manner hereinafter contained.

3. All sums found due to the KILA under or by virtue of this agreement shall be recoverable from the bounden and his properties movable and immovable under the provisions of the Revenue Recovery Act for the time being in force as though such sums are arrears of land revenue and in such other manner as the Director may deem fit.

In witness whereof Shri. (H.E. name and designation) for and on behalf of the KILA and Shri. the bounden have hereunto set their hands the day and year shown against their respective signatures.



Document 2017/101/12083 - GENERAL - File No. 2017/101/3339
Approved by Director on 02/11/2017 20:50:10

<http://www.kila.ac.in>
UcwhB-NrH-ocqFH-di.mzN



KILA, Mulankunathukavu, Thrissur

Signed by Shri.(date)

In the presence of witness:

1.
2.

Signed by Shri. (date)

In the presence of witness:

1.
2.



KILA, Mulankunnathukavu, Thrissur

Special Conditions

1. The selected supplier should arrange for a demonstration showing all the features listed in the technical specification. Supply order will be issued only after the acceptance of the product after the demonstration .
2. The Report / Proofs (if any) for the Certificates which listed in the technical specification should be submitted along with the tender.
3. Installation of Endpoint Protection Solution is the sole responsibility of Supplier concerned.
4. Supplier should provide necessary training relating to the installation and configuration of Endpoint Protection Solution to the System Administrator.
5. Brochures and all technical literature of the Endpoint Protection Solution should be enclosed along with the tenders submitted.
6. User Manuals (if any) should be handed over to KILA during the time of installation.
7. Maximum delivery period for the items in the purchase order will be two weeks from the receipt of purchase order by the supplier.
8. Failure to supply and install items within the specified time as per the agreement, a penalty of one percent of the item per week will be levied. (The time will be extended only with the prior concurrence from KILA).
9. Price quoted should be valid until tenders are processed. The tenders submitted without fulfilling the conditions as stated will be summarily rejected.
10. **The rate quoted should be for delivery, installation and training to the System Administrator at KILA. The items should be delivered installed within two weeks from the date of receipt of the purchase order. The rates should be inclusive of all taxes, duties etc (if any).**
11. The tenders should be accompanied by an agreement executed and signed in Kerala Stamp paper of Rs.200/- and an amount equal to 1% of the total cost of the articles tendered for as Earnest Money Deposit in the form of crossed Demand Draft drawn in favour of 'The Director, Kerala Institute of Local Administration' payable at Thrissur.

Cost of Tender form	: Rs.500 /- +GST
Last date of sale of tender form	: 15.11.2017 1 PM
Last date of receipt of tender	: 15.11.2017 3 PM
Date of opening the tender	: 15.11.2017 3.30 PM

Address to which tenders are to be submitted :

The Director,
Kerala Institute of Local Administration (KILA),
Mulankunnathukavu P.O.,
Thrissur - 680581.

Director, KILA

Signature of the Tenderer

OFFICE SEAL



Technical Specification for EndPoint Protection Solution

Sr.No.	Description
1	
2	Solution should able to Detects and blocks malicious software in real time, including viruses, worms, Trojan horses, spyware, Adware, and RootKit.
3	The Antivirus solution must automatically scan external devices (Floppy disks, Compact disks, USB devices and Network shares in real-time when accessed) as soon as they are attached to PC, Server, Laptop etc.
4	Anti-Virus Software must have the capability to clean, Quarantine or delete Viruses and should be able to detect new classes of viruses by normal virus definition update mechanisms
5	The Antivirus Solution technology should include a behavioral based technology apart from providing the signatures for vulnerability add heuristic based approach. It should be able to score both good and bad behaviors of unknown applications, enhancing detection and reducing false positives without the need to create rule-based configurations to provide protection from unseen threats i.e. zero-day threats.
6	The Antivirus solution must scan compressed file formats like ZIP, ARJ GZIP, BZ2,JAR,, RAR,LHZ,TAR Microsoft compressed tile etc.
7	The Antivirus solution Should have a Centralized Management Console & Shall manage the anti-virus programs on the network from a single web-based console.
8	Antivirus Solution should be capable of deploying Antivirus on all desktop and servers attached to the network centrally.
9	Antivirus should also able to generate the information reports such as Antivirus coverage, Virus definition update. Virus infection detected and action performed etc.
10	The Antivirus solution must provide a mechanism for developing and deploying policy to each system! node with respect to scheduling scan jobs, real-time scan settings, signature distribution, alerting and analysis etc.
11	The Antivirus solution Should Support Multi -Platform operating system(Windows , Mac, Linux) and the same should be managed from a single Centralised Management cosole
12	Antivirus solution should support integration with Active directory for directory structure of computers for better management & Should have logical group based on IP addresses (Subnets),
13	Antivirus solution Should have a Single, Configurable Installation with centralized configuration & policy management & Should have a Common Distribution Mechanism via combination of push & pull Technology for better BW management



Sr.No.	Description
14	Anti virus Should be capable of pushing client installation from a centralized location and it should also support manual installation of client Via network share .
15	Automatic update of Antivirus Server from Vendor Site & client should get update from the local Server & If updating from the Primary Server fails for any reason (such as the user being off the network) an attempt should be made to contact the Secondary Server (I.e Vendor site)
16	Antivirus should provide centralized event logging to locate and cure virus problems.
17	Administrator Should be able to initiate virus sweeps remotely in case of an outbreak.
18	Administrator should have flexibility to schedule Scan and update at the endpoints from central Server.
19	Administrator must be able to distribute new and update anti-virus software, virus definitions and Policies automatically to clients and servers from a central location .
20	Antivirus should provide a feature for the roll back of malware actions during disinfection(Roll back means rolling back the changes made to the file system (creating, relocating,renaming files) and registry keys
21	Solution should have File antivirus with following technologies a) Signature based analyses b) heuristic based analyses c) iSwift & ichecker based scanning
22	Solution should provide Web antivirus features which should analyse site address and block access to dangerous sites & Scan the object downloaded over HTTP
23	Solution should provide Mail antivirus features which:
	23a. should protect from the threats that e-mail message may contain & Meessages should be intercepted at the protocol level and by embedding into the most popular mail clients.
	23b. should provide scanning capabilities for POP3, SMTP, NNTP and IMAP mail traffic, protecting email communications from one of the most common channels of malware attack
24	Solution should provide IM antivirus features which should protect from the threats that IM attachment may contain & and it should support the following Instant mesaging applications: ICQ,MSN,AIM,MAIL.RU AGENT & IRC
25	Solution should provide a web console feature that works via a browser (The websole should be used for creating reports and performing simple operations with computers I.e viewing the status,relocating,Installing Antivirus
26	Solution should provide Application Privilege Control to regulate the activities of the running programs, namely, access to the file system and registry as well as interaction with other programs.



Sr.No.	Description
27	The Firewall module should have rule-base approach, with administrator defined rules
28	The Firewall module should have feature to allow or block certain network traffic, based on port-number / protocol and based on network address.
29	The Firewall module should monitor the traffic from the applications installed on that endpoint. Specific rules can be created to block certain applications's network traffic.
30	The solution should have HIPS module, which could protect the endpoint from network based attacks. The signatures for HIPS should be regularly updates to identify latest network attacks for endpoints.
31	The endpoint solution should have a feature to detect network attacks originating from a computer, and then block the traffic from that computer.
32	The Firewall module should have option to create network subnets like Public, Trusted, Local etc, and accordingly the network traffic flowing rules should be created.
33	The firewall module should have option to automatically categorize the applications in Trusted, Low Restricted, High Restricted, Untrusted etc, and accordingly the application's network traffic should be allowed
34	Firewall should allow creation of inbound or outbound traffic restriction rules
35	Antivirus Solution should provide Application Control module with Following:
	35a. Application categorization
	35b. Dynamic Whitelisting database consisting of programs that are constantly scrutinized to ensure they are legitimate
	35c. Golden Image support
	35d. Default deny' support
	35e. Trusted updater' support
36	Antivirus Solution should provide Device-control module with Following:
	36a. ability to control usage of unknown or unwanted devices, reducing the risk of data loss
	36b. White list categories (based on serial numbers)
	36c. Temporary grant access to block device over the Internet
	36d. Device inventory
37	Antivirus Solution should provide Web control module with following:
	37a. URL filtering and categorisation
	37b. Access scheduling
	37c. Blocking by data type
	37d. Blocking by content
	37e. Web Action like Allow, Block & Warn
	37f. Integration with Active Directory for Users and Groups
38	Antivirus should have Exploit Prevention which when detects any suspicious behaviour. the application will be blocked & report same to Server.



Sr.No.	Description
39	Solution should provide tamper protection features i.e user who does not know the password may not be able to change the existing policy, exit or uninstall the antivirus solution.
40	The proposed solution should have Predefined rules for hundreds of the most commonly used applications reduce time spent on configuring the firewall
41	Alerts on virus activity should be passed on to administrator
42	Solution should provide Mobile device security & Mobile device Management (MDM) feature & it should support Active Directory, Microsoft Exchange ActiveSync and Apple MDM Server.
43	Solution should provide management visibility and security for mobile endpoints — without the complexity of a separate solution.
44	Solution should provide Antimalware feature for Mobile devices and should use the power of the cloud to provide rapid protection against new and emerging threats.
45	Solution should provide Multi-level defence technologies for mobile devices (E.g. Anti-spam technology to filter out unwanted calls and text messages) it should also have Safe Browser feature for iOS devices to protect against phishing websites.
46	Solution should have feature to Enforce encryption on each user's mobile device and should offer a convenient way to enforce the use of the encryption technologies that are resident within the mobile device – so we can easily ensure that all data on the device is encrypted or just encrypt all of the corporate data that's held within a special container on the user's device.
47	Solution should support Bring Your Own Device (BYOD) initiatives and should include containerisation features – to help ensure corporate data and personal data are held in separate containers on the user's device.
48	Solution should have special Anti-theft features that should help to minimise the risk of security breaches that can result from a lost or stolen device.
49	Solution should have Remote Lock, Find and Wipe features (E.g. Administrator can remotely lock a mobile device, find the device's approximate location he can also choose to wipe corporate data from the device and return the device to its original factory settings.
50	Solution should have a feature which can help administrator in Controlling a lost device... even when its SIM has been changed
51	Solution should have a Mobile device management (MDM) feature with extensive mobile device management functionality – to give administrator easy and rapid control over all mobile security functions.
52	Solution should have boosting systems management capabilities plus an array of security technologies that can be managed and controlled from one management console.



Sr.No.	Description
53	Solution should have a feature for the creation and cloning of computer images – to save time and help to optimise operating system deployment. Images should be stored in a special inventory and it should be ready for access during deployment.
54	Solution should have a Application provisioning feature E.g. Administrator can deploy third party software on command or can schedule it for outside normal office hours. The software deployment process should be entirely transparent to users.
55	Solution should have a License Provisioning and Control feature (E.g. centralised licence provisioning and tracking of any breaches of licence conditions)
56	Solution should have Asset management feature – hardware & software (E.g. all devices and software on the network should be automatically discovered and recorded in hardware and software inventories.)
57	Solution should have Patch Management features - Advanced in-depth scanning for vulnerabilities combined with the automated distribution of patches.
58	Solution should have a Remote troubleshooting and deployment tool I.e it should help administrator to resolve problems efficiently. Furthermore, when he need to deploy new software at a remote office, he can reduce the load on his network by using one local workstation as the update agent for the whole site.
59	Solution should have option to integrate with SIEM systems like, HP ArcSight & IBM QRadar
60	Solution should have full-disk , file level & removable media backed by Advanced Encryption Standard (AES) with 256 bit encryption to secure critical business information in the event of device theft or loss.
61	Full Disk Encryption should operate on the physical sectors of the disk – to deliver encryption that’s ‘close to the hardware’ and also enable an ‘encrypt everything at once’ strategy.
62	File level Encryption should offer granular encryption of individual files and helps to enable secure sharing of data across your network.
63	Solution should have a feature to Increase security through policies that enforce the encryption of data on removable devices.
64	Solution should support Portable Mode for File Level Encryption on removable media
65	Users can create password-protected, encrypted, self-extracting packages of files and folders. This enables the secure transfer and sharing of sensitive data – via a removable device, email or the web.
66	Administrator should be able to access vital encrypted data in the event of a system failure – even if the operating system is unable to boot.



Sr.No.	Description
67	If a user loses or forgets their password, a challenge / response mechanism should allow the recovery of the pre-boot password to access the encrypted data
68	Vendor Should have 24x7 anti-malware laboratory analysis centers to provide proactive rapid protection against known and unknown threats
69	Vendor should be ICSA (International computer security association), Check Mark(West coast Labs) , VB 100 certified.
70	Vendor should be Top Rated Products for last 3 years in AV Comparatives Test
71	Proposed Solution should be a ' Leader ' in the Magic Quadrant for Endpoint protection Platform.



Tender Schedule

Sr. No	Description	Compliant / Non Compliant	Remarks
1	The Antivirus solution should provide enhanced antivirus protection for desktops, laptops & servers of all the attacks originating from places inside/outside of the network due to virus and/or other malicious programming code and should give appropriate warning messages	Yes/ No	
2	Solution should able to Detects and blocks malicious software in real time, including viruses, worms, Trojan horses, spyware, Adware, and RootKit.	Yes/ No	
3	The Antivirus solution must automatically scan external devices (Floppy disks, Compact disks, USB devices and Network shares in real-time when accessed) as soon as they are attached to PC, Server, Laptop etc.	Yes/ No	
4	Anti-Virus Software must have the capability to clean, Quarantine or delete Viruses and should be able to detect new classes of viruses by normal virus definition update mechanisms	Yes/ No	
5	The Antivirus Solution technology should include a behavioral based technology apart from providing the signatures for vulnerability add heuristic based approach. It should be able to score both good and bad behaviors of unknown applications, enhancing detection and reducing false positives without the need to create rule-based configurations to provide protection from unseen threats i.e. zero-day threats.	Yes/ No	
6	The Antivirus solution must scan compressed file formats like ZIP, ARJ GZIP, BZ2,JAR,, RAR,LHZ,TAR Microsoft compressed tile etc.	Yes/ No	
7	The Antivirus solution Should have a Centralized Management Console & Shall manage the anti-virus programs on the network from a single web-based console.	Yes/ No	
8	Antivirus Solution should be capable of deploying Antivirus on all desktop and servers attached to the network centrally.	Yes/ No	
9	Antivirus should also able to generate the information reports such as Antivirus coverage, Virus definition update. Virus infection detected and action performed etc.	Yes/ No	



10	The Antivirus solution must provide a mechanism for developing and deploying policy to each system! node with respect to scheduling scan jobs, real-time scan settings, signature distribution, alerting and analysis etc.	Yes/ No	
11	The Antivirus solution Should Support Multi -Platform operating system(Windows , Mac, Linux) and the same should be managed from a single Centralised Management cosole	Yes/ No	
12	Antivirus solution should support integration with Active directory for directory structure of computers for better management & Should have logical group based on IP addresses (Subnets),	Yes/ No	
13	Antivirus solution Should have a Single, Configurable Installation with centralized configuration & policy management & Should have a Common Distribution Mechanism via combination of push & pull Technology for better BW management	Yes/ No	
14	Anti virus Should be capable of pushing client installation from a centralized location and it should also support manual installation of client Via network share .	Yes/ No	
15	Automatic update of Antivirus Server from Vendor Site & client should get update from the local Server & If updating from the Primary Server fails for any reason (such as the user being off the network) an attempt should be made to contact the Secondary Server (I.e Vendor site)	Yes/ No	
16	Antivirus should provide centralized event logging to locate and cure virus problems.	Yes/ No	
17	Administrator Should be able to initiate virus sweeps remotely in case of an outbreak.	Yes/ No	
18	Administrator should have flexibility to schedule Scan and update at the endpoints from central Server.	Yes/ No	
19	Administrator must be able to distribute new and update anti-virus software, virus definitions and Policies automatically to clients and servers from a central location .	Yes/ No	
20	Antivirus should provide a feature for the roll back of malware actions during disinfection(Roll back means rolling back the changes made to the file system (creating, relocating,renaming files) and registry keys	Yes/ No	
21	Solution should have File antivirus with following	Yes/ No	



	technologies a) Signature based analyses b) heuristic based analyses c) iSwift & ichecker based scanning		
22	Solution should provide Web antivirus features which should analyse site address and block access to dangerous sites & Scan the object downloaded over HTTP	Yes/ No	
23	Solution should provide Mail antivirus features which:	Yes/ No	
	23a. should protect from the threats that e-mail message may contain & Messages should be intercepted at the protocol level and by embedding into the most popular mail clients.	Yes/ No	
	23b. should provide scanning capabilities for POP3, SMTP, NNTP and IMAP mail traffic, protecting email communications from one of the most common channels of malware attack	Yes/ No	
24	Solution should provide IM antivirus features which should protect from the threats that IM attachment may contain & and it should support the following Instant messaging applications: ICQ,MSN,AIM,MAIL.RU AGENT & IRC	Yes/ No	
25	Solution should provide a web console feature that works via a browser (The websole should be used for creating reports and performing simple operations with computers I.e viewing the status,relocating,Installing Antivirus	Yes/ No	
26	Solution should provide Application Privilege Control to regulate the activities of the running programs, namely, access to the file system and registry as well as interaction with other programs .	Yes/ No	
27	The Firewall module should have rule-base approach, with administrator defined rules	Yes/ No	
28	The Firewall module should have feature to allow or block certain network traffic, based on port-number / protocol and based on network address.	Yes/ No	
29	The Firewall module should monitor the traffic from the applications installed on that endpoint. Specific rules can be created to block certain applications's network traffic.	Yes/ No	
30	The solution should have HIPS module, which could protect the endpoint from network based attacks. The signatures for HIPS should be regularly updates to identify latest network attacks for endpoints.	Yes/ No	



31	The endpoint solution should have a feature to detect network attacks originating from a computer, and then block the traffic from that computer.	Yes/ No	
32	The Firewall module should have option to create network subnets like Public, Trusted, Local etc, and accordingly the network traffic flowing rules should be created.	Yes/ No	
33	The firewall module should have option to automatically categorize the applications in Trusted, Low Restricted, High Restricted, Untrusted etc, and accordingly the application's network traffic should be allowed	Yes/ No	
34	Firewall should allow creation of inbound or outbound traffic restriction rules	Yes/ No	
35	Antivirus Solution should provide Application Control module with Following:	Yes/ No	
	35a. Application categorization	Yes/ No	
	35b. Dynamic Whitelisting database consisting of programs that are constantly scrutinized to ensure they are legitimate	Yes/ No	
	35c. Golden Image support	Yes/ No	
	35d. Default deny' support	Yes/ No	
	35e. Trusted updater' support	Yes/ No	
36	Antivirus Solution should provide Device-control module with Following:	Yes/ No	
	36a. ability to control usage of unknown or unwanted devices, reducing the risk of data loss	Yes/ No	
	36b. White list categories (based on serial numbers)	Yes/ No	
	36c. Temporary grant access to block device over the Internet	Yes/ No	
	36d. Device inventory	Yes/ No	
37	Antivirus Solution should provide Web control module with following:	Yes/ No	
	37a. URL filtering and categorization	Yes/ No	
	37b. Access scheduling	Yes/ No	
	37c. Blocking by data type	Yes/ No	
	37d. Blocking by content	Yes/ No	
	37e. Web Action like Allow, Block & Warn	Yes/ No	
	37f. Integration with Active Directory for Users and Groups	Yes/ No	
38	Antivirus should have Exploit Prevention which	Yes/ No	



	when detects any suspicious behaviour. the application will be blocked & report same to Server.		
39	Solution should provide tamper protection features i.e user who does not know the password may not able to change the existing policy, exit or uninstall the antivirus solution.	Yes/ No	
40	The proposed solution should have Predefined rules for hundreds of the most commonly used applications reduce time spent on configuring the firewall	Yes/ No	
41	Alerts on virus activity should be passed on to administrator	Yes/ No	
42	Solution should provide Mobile device security & Mobile device Management (MDM) feature & it should supports Active Directory, Microsoft Exchange ActiveSync and Apple MDM Server.	Yes/ No	
43	Solution should provide management visibility and security for mobile endpoints — without the complexity of a separate solution.	Yes/ No	
44	Solution should provide Antimalware feature for Mobile devices and should use the power of the cloud to provide rapid protection against new and emerging threats.	Yes/ No	
45	Solution should provide Multi-level defence technologies for mobile devices (E.g. Anti-spam technology to filter out unwanted calls and text messages) it should also have Safe Browser feature for iOS devices to protect against phishing websites.	Yes/ No	
46	Solution should have feature to Enforce encryption on each user's mobile device and should offer a convenient way to enforce the use of the encryption technologies that are resident within the mobile device – so we can easily ensure that all data on the device is encrypted or just encrypt all of the corporate data that's held within a special container on the user's device.	Yes/ No	
47	Solution should support Bring Your Own Device (BYOD) initiatives and should include containerisation features – to help ensure corporate data and personal data are held in separate containers on the user's device.	Yes/ No	
48	Solution should have special Anti-theft features that should help to minimise the risk of security breaches that can result from a lost or stolen device.	Yes/ No	
49	Solution should have Remote Lock, Find and Wipe	Yes/ No	



	features (E.g. Administrator can remotely lock a mobile device , find the device's approximate location he can also choose to wipe corporate data from the device and return the device to its original factory settings.		
50	Solution should have a feature which can help administrator in Controlling a lost device... even when its SIM has been changed	Yes/ No	
51	Solution should have a Mobile device management (MDM) feature with extensive mobile device management functionality – to give administrator easy and rapid control over all mobile security functions.	Yes/ No	
52	Solution should have boosting systems management capabilities plus an array of security technologies that can be managed and controlled from one management console.	Yes/ No	
53	Solution should have a feature for the creation and cloning of computer images – to save time and help to optimise operating system deployment. Images should be stored in a special inventory and it should be ready for access during deployment.	Yes/ No	
54	Solution should have a Application provisioning feature E.g. Administrator can deploy third party software on command or can schedule it for outside normal office hours.The software deployment process should be entirely transparent to users.	Yes/ No	
55	Solution should have a License Provisioning and Control feature (E.g. centralised licence provisioning and tracking of any breaches of licence conditions)	Yes/ No	
56	Solution should have Asset management feature – hardware & software(E.g. all devices and software on the network should be automatically discovered and recorded in hardware and software inventories.)	Yes/ No	
57	Solution should have Patch Management features - Advanced in-depth scanning for vulnerabilities combined with the automated distribution of patches.	Yes/ No	
58	Solution should have a Remote troubleshooting and deployment tool I.e it should help administrator to resolve problems efficiently. Furthermore, when he need to deploy new software at a remote office, he can reduce the load on his network by using one local workstation as the update agent for the whole site.	Yes/ No	
59	Solution should have option to integrate with SIEM systems like, HP ArcSight & IBM QRadar	Yes/ No	



60	Solution should have full-disk , file level & removable media backed by Advanced Encryption Standard (AES) with 256 bit encryption to secure critical business information in the event of device theft or loss.	Yes/ No	
61	Full Disk Encryption should operate on the physical sectors of the disk – to deliver encryption that’s ‘close to the hardware’ and also enable an ‘encrypt everything at once’ strategy.	Yes/ No	
62	File level Encryption should offer granular encryption of individual files and helps to enable secure sharing of data across your network.	Yes/ No	
63	Solution should have a feature to Increase security through policies that enforce the encryption of data on removable devices.	Yes/ No	
64	Solution should support Portable Mode for File Level Encryption on removable media	Yes/ No	
65	Users can create password-protected, encrypted, self-extracting packages of files and folders. This enables the secure transfer and sharing of sensitive data – via a removable device, email or the web.	Yes/ No	
66	Administrator should be able to access vital encrypted data in the event of a system failure – even if the operating system is unable to boot.	Yes/ No	
67	If a user loses or forgets their password, a challenge / response mechanism should allow the recovery of the pre-boot password to access the encrypted data	Yes/ No	
68	Vendor Should have 24x7 anti-malware laboratory analysis centers to provide proactive rapid protection against known and unknown threats	Yes/ No	
69	Vendor should be ICISA (International computer security association), Check Mark(West coast Labs) , VB 100 certified. (Attach relevant certificates / proof)	Yes/ No	
70	Vendor should be Top Rated Products for last 3 years in AV Comparatives Test (Attach relevant certificates / proof)	Yes/ No	
71	Proposed Solution should be a ' Leader ' in the Magic Quadrant for Endpoint protection Platform. (Attach relevant certificates / proof)	Yes/ No	

Note : Strike out which ever is not applicable. The default answer will be NO, if no answer is updated on this field



Document 2017/101/12083 - GENERAL - File No. 2017/101/3339
Approved by Director on 02/11/2017 20:50:10

<http://www.kila.ac.in>
UcwhB-NrH-ocqFH-di.mzN



KILA, Mulankunathukavu, Thrissur