



Telangana State Technology Services Ltd.,

1st Floor, BRKR Bhavan, C-Block, Tankbund Road,
Hyderabad – 500063, Telangana State, India.

Phone: (40)23224935, 23226970; **Fax:** 23227458

Email: mngdirector-tsts@telangana.gov.in

Website: <http://www.tsts.telangana.gov.in>

CIN No: U74900TG2015SGC101517

Tender Ref. :TSTS/IIP/020/ITE&C-SOFT/2016-Refloat

Dated : 12.09.2017

To

SHORT TENDER NOTICE TO VENDORS

Sub: TSTS-IIP Division- Supply & Installation of Antivirus Software to ITE&C Department, Govt. of Telangana– Reg.

TSTS invites bids for Supply & Installation of Antivirus Software to ITE&C Department, Govt. of Telangana as per the details given in the Annexure

Last date and time for receipt of quotations: 16/09/2017 03:00 PM

Date and Time for opening of quotations :16/09/2017 03:30 PM

Tender document fee Rs.1000/- (DD should be drawn in favor of The MD, TSTSL)

Bidder who not paid document fee, EMD and Bids received after the due date and time for any reason whatsoever shall not be considered for opening.

Bids are to be submitted at O/o the TSTS, BRKR Bhavan, 1st Floor, Tank Bund Road, 'C' Block, Hyd.

1. For each quotation, **two separate sealed covers** should be submitted. One cover containing Pre-Qualification, Technical details (**PQ&TQ Bid**) and **another cover containing financial details (Financial Bid)**. Use the format Financial Bid Annexure -II. EMD & document purchase receipt details should be enclosed with the technical bid only
2. Quotation should be valid at least for a period of 30 days from the date of opening.
3. The unit price and total price should be mentioned separately exclusive of taxes and inclusive of taxes but in both cases inclusive of installation and other charges if any.
4. For any delays in delivery beyond delivery period mentioned in the purchase order, the bidder will be liable for penalties as mentioned in Clause 16.
5. i) The bidder should submit EMD equivalent to an amount as mentioned in the Annexure in the form of DD/BG from a Nationalized/Scheduled bank in favour of "The Managing Director, T.S. Technology Services Ltd.," Rotational BG is not acceptable.
ii) EMD will be returned to the unsuccessful bidders after finalization of the tender
6. The EMD should be valid at least for a period of 90 days from the date of opening of Technical bids.
7. If the bidder wants to give option, he may submit it as separate bid along with Separate EMD. This will be treated as a separated bid for evaluation.
8. Bidders must submit details of EMD value and date of validity along with their technical bid failing which the quotation is liable for rejection.
9. Conditional bids are not acceptable
10. Bidder has to quote for all items mentioned in the tender Schedules.
L-1 will be arrived for evaluation of overall the items mentioned in the tender. The bid will be rejected if the bidder has not quoted for all the items.
11. Any deviations in format may make the quotation liable for rejection.
12. Managing Director, TSTS reserves the right to accept or reject any or all the quotations without assigning any reasons thereof and to add, modify or delete any of the terms and conditions without any notice.
13. Managing Director , TSTS reserves the right to modify the technical specifications including quantity at any time during the process of finalization of tender
14. **Payment terms:**
- 14a. **Computers /Notebooks /Printers/UPS/Network/Projectors & Other Items**
 - i) 90 % payment on delivery & successful installation of systems duly deducting penalties if any
 - ii) 10 % payment after 30 days from the date of successful Installation and satisfactory certificate duly certified by the department official.
 - iii) In case Site not ready –75% on total value of that item and on submission of certificate from user Department.

15. **Installation :**
- i) PO consisting of 1-5 locations , bidder has to install the equipment or has to obtain Site Not Ready Certificate (where ever Site is Not Ready) from User Department officials within week days from the due date of Delivery.
 - ii) PO consisting of more than 5 locations , bidder has to install the equipment or has to obtain Site Not Ready Certificate (where ever Site is Not Ready) from User Department officials within in 2 weeks from the due date of Delivery.
16. **Penalty for late Delivery:**
For any delay in delivery, the Bidder will be liable for penalties as follows:
- i) 1% of the late delivered goods for One week or part thereof; 1.5%, for Two weeks or part thereof; 2% for Three weeks or part thereof and so on if it is less than Eight weeks, if it is more than Eight weeks the penalty will be compounded.
 - ii) If any delay is for more than 30 days, TSTS will reserve the right to cancel the order without giving any notice and EMD will be liable for forfeiture.
17. After delivery & installation of the equipment
- a) TSTS will conduct AT.
 - b) TSTS will also conduct 2nd AT if there are any shortfalls, remarks in the first AT. In this case an amount of Rs 2,000/- per visit per location will be charged to bidder account and same will be deducted from the amount Payable to the bidder.
18. NOTE:-A signed undertaking from the bidder certifying that all the Components / Parts / assembly used in the supplied items should be original new components / parts / assembly and that no refurbished / duplicate / second hand components / parts / assembly / Software's are used are or shall be used, has to be enclosed to the bid. Sample format is enclosed.

Yours Sincerely,


Manager (IP & NW)

Pre- qualification conditions

1. The bidder should have Cumulative Annual Turnover 20 sales of Software products for last two financial years, i.e. Years 2014-2015 & 2015-2016. (Note-The bidder must enclose proof documents i.e., purchase orders/Contract agreement etc., or Chartered Accountant certificate /Balance Sheet in support of their claim).
2. The Bidder should have minimum one Service center with or one authorized service person in Hyderabad as on bid calling date. Details of the service centers or service personnel should be enclosed in Form P4.
3. The bidder should furnish the information on major past client details.
4. The bidder should to submit PAN, GST details in the PQ Bid.
5. The bidder should be a manufacturer/ authorized representative of a manufacturer/whole sale dealer and should be in business of manufacture and or supply and maintenance of the offered items for a minimum period of Two years in TS/AP as on bid calling date. (The Manufacturer's Authorization for specific to this tender should be submitted as per the Annexure-III for Antivirus product). Non submission of MAF treated non responsive and disqualified.
6. The Bidder should give a Declaration that the Bidder has not been debarred/ blacklisted by any Central or State Govt. / Quasi –Govt. Departments or organizations for non-satisfactory past performance, corrupt, fraudulent or any other unethical business practices as per Format given in Form T2.

Note : Relevant documents in support of above should be furnished.

Tender Ref. TSTS/IIP/020/ITE&C-SOFT/2016-Refloat

Sub: Undertaking of authenticity for the offered items in the tender

This has reference to the Items being supplied mentioned in the tender and quoted vide our quotation no/invoice no. _____ dated _____.

- 1) We hereby undertake that all the goods/components/parts quoted in the tender shall be original new goods/components/parts from respective OEMs of the products and that no refurbished/duplicate/second hand components/parts assembly/software are being used or shall be used. Should you require, we shall produce certificate from our OEM supplier in support of above undertaking at the time of delivery. It will be our responsibility to produce such letters from our OEM supplier's within a reasonable time. In case we are found not complying with above at the time of delivery or during installation, for the items quoted /supplied in the tender already billed, we agree to take back and return the money if any paid to us by you in this regard.

Authorized Signatory
Name
Designation

**Tender Ref TSTS/IIP/020/ITE&C-SOFT/2016-Refloat
Form T2- Declaration Regarding Clean Track Record**

To,
The Managing Director
Telangana State Technology Services Limited
1st Floor, B Block, BRKR Bhavan,
Tankbund Road,
Hyderabad 500063, Telangana State, India

Sir,

I have carefully gone through the Terms & Conditions contained in the RFP Document [No. _____]. I hereby declare that my company has not been debarred/ black listed as on Bid calling date by any State Government, Central Government, Central & State Govt. Undertakings/enterprises/Organizations and by any other Quasi Government bodies/Organizations, World Bank and any other major Enterprise/Organizations in India for non-satisfactory past performance, corrupt, fraudulent or any other unethical business practices. Further, declaring that no cases pending against the firm/organization either in Government (State or Union) or as mentioned above for involvement in cases for supply of sub-standard goods/material or track record of supply of inferior quality or no enquiries on past supplies are being conducted or underway. I further certify that I am competent officer in my company to make this declaration.

Yours faithfully,

(Signature of the Bidder)
Printed Name
Designation
Seal
Date:
Business Address:

Tender Ref. TSTS/IIP/020/ITE&C-SOFT/2016-Refloat

Annexure-III- Manufacturer Authorization Format(MAF)

The authorization should be tender specific may be in the nature of a letter, memorandum or certificate regularly granted by the manufacturer to its channel partners, authorized solution providers, system integrators, distributors, etc. or a specific letter issued for purposes of this bid. Such communication should include statements / undertakings from the said manufacturer to the following effect.

- Guarantee and warranty coverage in respect of the goods and services manufactured by the said manufacturer shall be honored by that manufacturer, their channel partners, distributors, authorized service centers as the case may be.
- The manufacturer updates the bidder and their technical personnel with relevant technical literature, training and skill transfer workshops etc. on a regular basis.
- The manufacturer provide back to back technical support to the said bidder on a continuing basis.
- The said bidder is authorized to provide service and solutions using hardware, firmware and / or software as the case may be. Note: The letter of authority should be signed by a person competent and having the power of attorney to bind the manufacturer.

Date

Signature of Bidder & Seal

Tender Ref. TSTS/IIP/020/ITE&C-SOFT/2016-Refloat

Form-T1

Technical Deviation Statement

Sl. No.	Item	Specification Required	Specification of proposed item	Specification Higher/Lower

Date

Signature of Bidder & Stamp



Annexure-I

Tender Ref. TSTS/IIP/020/ITE&C-SOFT/2016-Refloat
Format for Technical BID

DELIVERY PERIOD	10 days	EMD Rs.	25,000/-
Delivery at	ITE&C Department, Hyderabad, GoTS		
VENDOR NAME			
Item No - 1	Renewal of Anti Virus	QUANTITY	1800 Nos.
		DEVIATIONS	
ITEMS		HIGHER	LOWER
Antivirus Protection			
	Renewal of exiting Quick Heal Total Security Antivirus Solutions for TSCAN, ITE&C Department. Part No:- QH-EPS-T regular		
1	Must offer comprehensive client/server security by protecting enterprise networks from viruses, Trojans, worms, hackers, network viruses, mixed threat attack from multiple entry points, and spyware.		
2	Have the capability to detect all in-the-wild viruses and Antivirus Engine should be certified with reputed VB100%, AV Comparitive, AV Test, ICSA Labs and Checkmark.		
3	Must have the capability to detect and block files with malicious executable content and embedded/compressed executables that use real-time compression algorithms.		
4	Must have the capability to detect and remove rootkits.		
5	Must have the capability to detect and quarantine suspicious files.		
6	Must have the capability to detect malware by behavioral detection techniques.		
7	Must have the capability to detect and remove roguewares.		
8	Must have the capability to identify source of infection i.e. from where the infection has originated in the network.		
9	Must have the capability to restore a file from quarantine if the file is deemed safe.		
10	Must provide Virus Outbreak Prevention mechanism, which should be activated based on threshold of detected malware.		
11	Should have anti malware protection and cleanup capability.		
12	Ordinary Users should not be able to modify AV settings except for those in special groups as deemed necessary by the Administrators.		
13	Update Managers: Should have the capability to create multiple update servers to distribute updates load in large network environment that reduce bandwidth consumed during definition updates.		
14	Must have the capability to perform different scan actions based on the virus type (Trojan/ Worm, Joke, Hoax, Virus, other)		
15	Must have the capability to scan compressed, archived, and packed files.		
16	Must have the capability to scan and disinfect infections from mobile phones.		
17	Must have the capability to scan plug and play USB storage drives as soon as they are connected.		
18	Must have the capability to terminate virus program threads in memory, repair registry, remove any malicious OS processes created by trojans.		
19	Must have the capability to disconnect infected endpoints from the network.		
20	Must have the capability to scan and repair OLE (Object Linking and Embedded) files.		
Device Control			

1	Must have the capability to grant allow, block, read-only access to various devices.
2	Must have the capability to grant access rights for storage devices such as USB, CD/DVD, Card Reader, etc.
3	Must have the capability to regulate the use of Wi-Fi and Bluetooth connections.
4	Must have the capability to retain control over interfaces such as Firewire Bus, Serial Port, SATA Controller, Thunderbolt, etc.
5	Must have the capability to control and regulate the use of printers, scanners, web cameras, and network shares.
6	Must have the capability to allow or block the attachment of Mobile Phones i.e. Android Phone, iPhone, iPad, & iPod etc to the endpoints.
7	Must have the capability to exclude any particular device from device control policies.
File activity monitoring	
1	Must have the capability to monitor activities related to file handling such as copy, delete, move on local drives, removable drives and network drives.
2	Must have the capability to monitor certain file types.
3	Must have the capability to exclude certain files/folders/paths from monitoring procedures.
Asset Management	
1	Must have the capability to collect system and hardware information related to remote endpoints.
2	Must have the capability to obtain a summary report of various software's/updates installed on endpoints.
3	Must have the capability to track software changes happening on endpoints i.e. applications installed/uninstalled.
4	Must have the capability to track hardware changes happening on endpoints. E.g. RAM Changed, Processor changed, etc.
IDS/IPS	
1	Must have the capability to detect, and prevent network based and host based intruder attempts on the home networks.
2	Must have the capability to prevent port scanning attacks.
3	Must have the capability to prevent DDOS attacks.
4	Must have the capability to generate reports for potential security breaches, policy violations, and suspicious traffic flow.
Web Security and Web Filtering	
1	Must have the capability to block user access to malicious and phishing websites from configured endpoints.
2	Must have the capability to block user access to websites based on their categories e.g. Social Networking, News, etc.
3	Must have the capability to block entire domain or a particular website/URL
4	Must have provision to exclude certain websites or entire domains.
5	Must have the capability to block https sites.
Application control	
1	Must be able to block applications based on application categories. E.g. Download Managers, File sharing applications, Games, etc.
2	Must have ability to add custom applications to the blocked application list.
3	Must have capability to collect list of all installed applications in the network.
Data Loss Prevention	
1	You can now prevent unauthorized, pilferage loss, or leakage of confidential company data using the data loss prevention (DLP) feature

Handwritten signature

2	The DLP feature stop any such unauthorized activity that is carried out through channels		
2.1	Print screen, Removable devices, Using network share,Using clip board ,Using Emails ,Web browsers		
Roaming Plat Form			
1	Roaming service allows interacting with EPS server via cloud when the clients are out side the organizational network. This allows the administrator to apply the policies, installation .		
Manging console through Cloud			
1	cloud is a web based portal that enables to centrally manage and monitor your Enterprise products from a remote location outside your organizational network.		
Firewall			
1	Must provide the flexibility to create firewall rules to filter connections by IP address, port number, or protocol, and then apply the rules to different groups of users.		
2	Must have the capability to examine and control all incoming and outgoing traffic per configured settings for ports, source, or origin or destination address.		
Email Protection			
1	Must have the capability to block infected and spam mails.		
2	Must have the capability to allow only trusted email clients to send mails.		
Groups and Policies			
1	Must have the capability to create multiple user groups as per organizational structure.		
2	Must have the capability to assign different policy configuration to each group.		
3	Must have the capability to import group structure from Active Directory.		
4	Must have the capability to import/export groups and policies.		
5	Must provide Policy deployment status (Applied, Pending or Failed) on EPS web console		
Client Deployment			
1	Must have the capability to deploy the Client software using the following mechanisms:		
1.1	Client Packager (Executable & Microsoft Installer (MSI) Package Format)		
1.2	Web install page		
1.3	Login Script Setup		
1.4	Remote installation on single endpoint or on entire IP range.		
1.5	From a client disk image		
1.6	Through Active Directory and by creating group policy object		
2	Client uninstallation should only be done by administrator.		
Management Features			
1	Must provide a secure GUI or Web-based management console to give administrators access to all clients and servers on the network for client administration.		
2	Must have the flexibility to roll back updates if required via the management console.		
3	Should have role based administration capability.		
4	Must support plug-in modules designed to add new security features without having to redeploy the entire solution, thereby reducing effort and time needed to deploy new security capability to clients and servers across the network		

Jh

5	EPS web console should support on Google Chrome, Internet Explorer and Mozilla Firefox Browsers.		
Notification, Reporting and logging			
1	Must provide email and sms notification for various critical events such as virus outbreak, license getting expired etc		
2	Must have the capability to generate a graphical as well as tabular reports.		
3	Must have capability to export reports in multiple formats such as PDF and CSV.		
4	Must have capability to automatically send the report to administrators email address as per configured schedule.		
5	Must have capability to automatically purge old reports after a preconfigured duration.		
6	Must have capability to log all activities of management server.		
Other features			
1	Must have the capability to prevent a user from accessing the operating system in safe mode.		
2	Must have the capability to improve performance of endpoints by cleaning junk files and deleting invalid registry/disk entries.		
3	Must support sandbox browsing for safe and secure browsing.		
4	Must have the capability to manage mobile workforce when they moves out of the corporate network.		
5	Must have the capability to identify and report vulnerabilities of installed applications and operating systems in the network.		
WARRANTY PERIOD COMPREHENSIVE IN YEARS		1 Year	
AMC PERCENTAGE BEYOND WARRANTY PERIOD(-----Specify----			
DELIVERY PERIOD IN DAYS		10 days	

Date

Signature of Vendor & Stamp

Annexure – II
Tender Ref. TSTS/IIP/020/ITE&C-SOFT/2016-Refloat
Format for FINANCIAL BID

Delivery	ITE&C Department, Hyderabad, GoTS		Delivery time	10 Days
VENDOR NAME				
ITEMS	Qty	Unit Price (Rs.)	Total Price (Rs.)	Warranty Period
Item No – 1 : Renewal of exiting Quick Heal Total Security Antivirus Solutions for TSCAN, ITE&C Department.	1800			1 Year
Grand Total				
Amount in words				

Date

Signature of Vendor & Stamp