Punjab State Power Corporation Limited

(Regd. Office :PSEB Head Office, The Mall Patiala – 147001,
Corporate Identity Number : U40109PB2010SGC033813 Website:www.pspcl.in

OFFICE OF THE CHIEF ENGINEER/GGSSTP,
MATERIAL MANAGEMENT CELL-II V&P.O. GHANAULI, ROOPNAGAR-140113
(FAX NO 01881-274232, PH NO 01881-275666)
(ISO 9001:2000 CERTIFIED)
e-mail : **se-hq-ggsstp-ropar@pspcl.in**

SHORT TERM BASIS

To

Regd./Email

Limited Tender enquiry,
On various firm`s as per overleaf.

Memo No. 1161/71 /P-2/EMP- 11943
Dated: 28/3/22

Subject:- Purchase of server based and standalone antivirus software to secure GGSSTP LAN and computer systems/ Laptops not connected over LAN.

Enquiry No. 7251 **/P-II/EMP-** 11943 **dated:** 28.3.22

Date & Time of Receipt of Tender 18.4.22 upto 11.00 A.M.

Date & Time of Opening of Tender 18.4.22 at 11.30 A.M.

(In case opening date happens to be holiday, tender shall be opened on next working date at the same time)

Dear Sirs,

Please send your sealed quotation in duplicate in the Performa attached on the firm prices for the supply and delivery of items as detailed in Annexure-'A' enclosed. Enquiry No. and date of opening of tender must be legibly mentioned at right top corner of sealed cover. General terms & conditions shall be as per Annexure-'B' attached. Your quotation should be in two parts. For each item, unit rates should be quoted strictly on the attached performa of pricing schedule. Please note that if quoted rates are not as per attached performa, the offer is liable to be rejected. Insurance and freight charges should be quoted separately.

Also please note that competent authority may distribute the quantities to be procured on more than one firm.

The offer must be kept valid for atleast 120 days

D/A- Annexure- A, B, Performa for Schedule of Deviation & Performa of pricing schedule & technical specifications

28/3/2022
O/C Dy CE./Hq.,
GGSSTP, Rupnagar

CC :-

1) Dy.C.E./EMC,GGSSTP,Rupnagar along with Annexure-A to check specifications and intimate, if there is any discrepancy please.
2) Dy CAO,GGSSTP,Rupnagar.
3) Notice Board

CP-5

PUNJAB STATE POWER CORPORATION LIMITED

(Regd. Office : PSEB Head Office, The Mall, Patiala – 147001 Corporate identity Number U40109PB2010SGC03381
Website: www.pspcl.in **OFFICE OF THE CHIEF ENGINEER /GGSSTP,**
MATERIAL MANAGEMENT CELL-2, V&P.O. GHANAULI, ROOPNAGAR-140113
Phone no. 01881-275666

Annexure-'A'

ENQUIRY NO. 7251 /P-II/EMP-11943 DT. 28·3·22

DETAIL OF MATERIAL AND TECHNICAL SPECIFICATIONS.

Sr.No.	GGSSTP Code	Description	Qty (Nos)
1.	TP045106	Server based antivirus software for 3 years.	110
2.	TP045110	Antivirus software for standalone computer system for 1 year	10

Note :- Technical Specifications are as per annexure – I attached.

Note:-

1) The rates quoted should be exclusive of GST. The firm should mention HSN code of each item & present rate of GST on each item
2) Firms should supply their GST Registration certificate along with offer/ Quotation.

Terms and Conditions:-

1) Fax/Telegraphic/e-mail tender shall not be accepted.
2) The tender shall be sent in two separate envelopes as under:-

(a) **Part-1**- One envelope containing deposit of Earnest Money (if applicable) & Technical /Commercial bids.

(b) **Part-2**- The other containing the prices.

While opening the tenders the envelope containing the Earnest Money (if applicable) & Technical /Commercial shall be opened first and in case the deposit of Earnest Money (if applicable) & Technical /Commercial is in accordance with the terms of notice inviting tender only then second envelope containing the tender (prices) shall be opened.

3) **The tender must be accompanied by EARNEST MONEY (If applicable as per Annexure-B)**

4) The rates should be quoted on FOR destination basis giving break up of FOR Destination price as per **Performa of pricing schedule** attached.

5) The Performa for price schedule enclosed with specification shall be filled by tenderers duly typed and **hand written prices shall not be accepted.**

6) In addition to the break-up of total price i.e. ex-works cost, GST, Freight, Insurance and Packing the bidders should also give split up of ex-works price.

7) **Split up of ex-works prices shall indicate cost of raw material, Labour component and overhead expenses.**

8) Raw material can further be divided into 3-4 parts depending upon type of material.

9) The offer should be kept valid for 120 days from date of opening of tenders.

10) The bidders are not allowed to indicate over all discounts on the quoted price for which split up has been given as mentioned in Sr. No. 6 & 7 above. However, quantity/payment discount can be given by the tenderer in the main tender.

11) Any firm offering discount on the quoted price or after the opening of tender will be out rightly rejected.

12) Competent authority may distribute the quantities to be procured on more than one firm.

13) All pages of quotation should be duly signed & stamped

14) Quantity can be increased or decreased.

15) Relevant literature/catalogue should be sent along with quotation.

16) **Negotiation shall not be held except with lowest bidder.**

17) Random testing of material on receipt in GGSSTP Store irrespective of the fact whether or not it was inspected before despatch shall be carried out by PSPCL. In case of any failure the entire lot shall be rejected at the risk and cost of the supplier.

18) Any deviation from PSPCL's standard terms and conditions be clearly mentioned in quotation under **"Schedule of deviations"** otherwise all terms and conditions will be deemed to have been accepted.

19) **Firm should mention GST number in their offer.**

20) The firm must mention HSN code of all items in their offer along with GST applicable on them. Uniform GST rates shall be applied while comparison of rates.

21) The location for the supply of goods/services must be in the territory of Punjab as goods are meant for use in Punjab.

22) Sourcing of service should be made from an agency with its office located in the territory of Punjab rather than merely from HQ of that agency. (which may be located outside the state).

23) **Tenders should enclose copies of Orders/Contracts against which they have supply same material to otherThermal Plants of other states.**

24) Any firm which at the time of opening of the Tender enquiry, falls in any of the following categories, shall be regarded as defaulter and shall not be eligible for participation in any new Tender enquiry for a period of three years from the date of issue of Purchase Order in which it has defaulted:-

a) The Firm is a defaulter for the supply of 35% or more quantity on the date of expiry of the Contractual Delivery Period for the total ordered quantity.

b) The Firm is a defaulter for the supply of any quantity for more than 6 months from the date of expiry of the Contractual Delivery Period for the total ordered quantity.

This clause shall be applicable item wise (all types, sizes and ratings) against which the firm has become defaulter under the above said conditions.

25) Payments can be made through RTGS system of Digital Payments instead of cheques to the suppliers/firms/contactors whosoever gives the consent. All the bank charges related to RTGS are to be borne by the suppliers/firms/contactors.

26) The firm whose manufacturing units are situated in State of Punjab shall be granted order preference to the extent of 50% of total value by de-escalating their rates by 15% in comparative statement on submission of undertaking enclosed on non-judicial stamp paper of appropriate value.

27) Firm which are registered with MSME are required to provide their registration certificate along with quotation. Please also note Clause no. 30(a) of Annexure-'B'

28) The firm should mention their complete address, official email id & contact no. in the quotation.

29) Conditional Tenders will not be accepted.

30) The quantity given in the NIT can be ordered upon more than one firms.

31) All other terms and conditions are as per Annexure - 'B' attached.

DA/ Annexure-B'

28/3/2022

Dy.CE/HQ,
GGSSTP, Roopnagar.

R

cp-3/1

Specifications of Antivirus Software

1. **Threat Detection**
   a. Antivirus
   b. Anti-spyware
   c. Email scanning
   d. Office documents scanning
   e. Always active protection
   f. Vulnerability scan
   g. Exploits protection
   h. Keylogger detection
   i. Unwanted Registry / Files/ Tracking Cookies Cleanup

2. **Web Protection**
   a. Safe Search (Cloud based annotation for search URLs)
   b. Safe Surf (Cloud based website verification and blocking for Phishing and Unsafe sites)
   c. Phishing site blocker
   d. Malicious site blocker
   e. Identity Protection (Automatic security prompt when Passwords are entered into non-secured sites)
   f. Category based web blocking

3. **Advanced PC Protection**
   a. System performance tune up
   b. USB Vaccination
   c. External Device Scanning
   d. External Device Blocking
   e. Anti-Spam
   f. Start-up apps manager
   g. Application control

4. **Internet Protection**
   a. Smart Firewall
   b. Intrusion Detection & Prevention
   c. Website Filtering
   d. Browser Protection

Note: The validity of Server Based Antivirus software and standalone antivirus should be for 3 years and one year respectively.

ASE/EM-2
GGSSTP. Roopnagar

3/2

Technical Specifications

Feature		Description	Compliance
		Management Console	
Enhanced Graphical Dashboard		The selected AV should have **Graphical Dashboard,** which should give immediate status of health of all client systems and highlights critical security situations that need immediate attention.	
Quickly Search		Quickly Search for a specific Computer / Threats/ Application / Website, when deployed to thousands of endpoints	
Performance		Less resource footage on endpoints, so maximum performance is assured even low configuration PCs also	
Easy Deployment and Maintenance	Remote Install	The selected AV should have Remote install – Installation via remote access of web console on any system in the network.	
	Notify Install	The selected AV should provide Installation via email notification (containing URL) for client installation.	
	Remote Uninstall	The selected AV should provide uninstallation via remote access of web console on any system in the network.	
Client Action	Remote Scan	The selected AV should have features to allow virus and malware scan of all networked computers from a central location.	
	Remote Update	Networked computers should be able to get updated from a central location.	
	Application Control	The selected AV should give Administrator the complete list of all applications installed in clients, also have provision to view the list of clients that are using a particular application. Administrator can enforce restrictions on clients for usage of a particular application with allow/block/allow internet access. Administrator can manually define rule to block an application with advanced settings and controls through application name or hashing technology.	
	Vulnerability Scan	The selected AV should scan for vulnerable applications installed in your network	

Regards

Group Policy Management	Manage Group	The selected AV should create, add, delete, rename Groups and sub groups to manage clients. All clients within a group share the same policy. You can also move clients from one group to another. You can also Pick & add particular group or client to move another group.	
	Manage Policies	These policies contain client settings for different groups in your organization.	
IDS/IPS & Zero Day Attack	IDS/IPS , Port Scanning Protection, DDOS Protection	The selected AV should effectively and efficiently filters unwanted traffic with advanced IPS and IDS functions	
Intelligent Firewall		The selected AV should blocks unauthorized access to business network. Allows customization rules to be set for LAN users and for roaming users (change automatically) for blocking ports/ inbound & outbound traffic with Severity Level of Low, high medium and also admin have provision to get log file report	
Vulnerability Scan		The selected AV should have Vulnerabilities scan, detects clients weakness by scanning the apps & win files which are prone to attacks. EPS also isolates a targeted attack also helps to take report on this	
Email Scan		The selected AV should effectively scans end-user inbound & outbound mail for malware	
Web Security	Browsing Protection	The selected AV should block malware infected and malicious websites.	
	Phishing Protection	The selected AV should block phishing websites.	
Web Filtering		The selected AV should allow blocking of more than 50 categories of websites (e.g. Botnet, cutting, Social Networking, etc.) or user-specified websites to limit web access and increase productivity also facility for Whitelist/Blacklist Custom Time Settings Exceptions	
Advance Storage & Device Control/Wifi restriction		The selected AV should control and configure various device types for Windows. Robust and flexible management options safeguard against unverified devices. This robust feature also facilitate prevents device access prevention like admin can black list or white list any USB based device in network and assign the same rule to Users wise or group wise , Also Access Restricted Wifi Access for laptop users in organization & Available with Password Protection for USB device	

Schedule	Client Scanning Schedule	The scans can also be scheduled at a specific time.	
	Vulnerability Scan	The Vulnerability Scan can also be scheduled at a specific time.	
	Update scheduling	The Automatic Update can also be scheduled at a specific time as specified by the admin.	
		Update size limit: Initial update should not be more than 200 MB and later on update/ incremental size should not more than 15 KB. Update process should not choke the branch intranet network bandwidth. The backend update process should not disturb the normal Working operation.	
Multiple Update Managers & Addon server		The product should be deployed as a single management console or as multiple management consoles or as add-on- server. This comes effective In a distributed network setup. The add-on server should hold AV installation packages.	
Reports	Export Report	Report should be able to exported and saved in a variety of formats (e.g. PDF, CSV).	
	Scheduling	Reporting should be scheduled according to the requirements over email	
	Event Logs of Server	Provide events logs of any activity done in Admin console.	
Asset Management		The selected AV should provide Complete Information about client Hardware details and throws notification to administrator even on the event of smallest change. Administrator can monitor hardware asset details of all PCs from the web console	
Update Manager		Should support multiple update manager to reduce network congestion for distributed network.	
Remote based policy management		Administrator should able to enforce policies, if the client is a roaming client. Admin and client should communicate with each other using private gateway.	
Email Notifications		The selected AV should have feature allowing notifications to be sent to configured email addresses and numbers alerting them of critical network events.	
Redirection of Specific Groups/Clients		Manually redirects specific client groups/clients to different servers to manage each client of AV.	

Regards

Roaming Client		The selected AV should allow user to take definition update via internet when he is not connected to intranet network without make any changes in settings.	
Easy Migration		Easy migration Antivirus Server. Automatic up gradation of Clients	
Easy Licensing		The selected AV should allow user to add additional client license to increase client support.	
		Client Features	
Core Protection	Antivirus	Antivirus, or AV software is a computer software used to prevent, detect and remove malicious computer viruses.	
	Anti Spyware	Antispyware software helps protect your computer against pop-ups, slow performance, and security threats caused by spyware and other unwanted software.	
	Anti Malware	Anti-malware will scan computers and systems against malware, including viruses, spyware and other harmful programs such as: computer viruses, malicious BHOs, hijackers, ransomware backdoors, rootkits, trojan horses, worms, malicious LSPs, dialers, fraud tools, adware and spyware.	
	AntiRootkit	A rootkit is a stealthy type of software, typically malicious, designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer.	
	Behaviour Detection system	enhanced to detect behavioral and characteristic inspection and monitoring of unsafe programs. This results in a clean, more up-to-date and accurate detection of threats.	
Improved Scan Engine		The revamped antivirus scan engine avoids rescanning files that have not been altered since the previous scan. This reduces system resource usage.	
	Browsing Protection	Internet security to web browsers in order to protect networked data and computer systems from breaches of privacy or malware	

3/4

Management & Policy over Ridge	Policy Over Ridge	This a global settings and older data can be purged Administrator can quickly implement any configuration changes globally across the computers using Policy Override without having to change all the policies.	
	Flash Drive Protection	Automatically scans external storage devices. Protects USB drives from auto run infections.	
Preventive Tools	Enhanced Self-Protection	The Self-protection feature now protects Antivirus running processes and services	
	Password Protection	Password protection is a security process that protects information accessible via computers that needs to be protected from certain users. Password protection allows only those with an authorized password to gain access to certain information.	
	Block Suspicious Files	Identify and block suspiciously files.	
	From Admin Server	Client Protection can take update from Admin server.	
Update	From Internet	Client protection can take update form internet, if system is not connected with intranet network.	
Scans	Full System Scan	Will scan complete system	
	Custom Scan	User can scan specific file or folder.	
	Memory Scan	It will help to scan memory of system.	
	Property Sheet Scanner	Property sheet scanner is shortest way to get maximum details of file.	
	Automatic Rogue ware Scan	That deceives or misleads users into paying money for fake or simulated removal of malware (so is a form of ransomware) — or it claims to get rid of, but instead introduces malware to the computer.	
	Exclude Files and Folders	Exclude file and folder from all scanning.	
	Exclude File extension	Exclude file extension from all scanning.	
	Silent Mode	Suppresses prompts across all Antivirus modules thereby reducing system load and allowing uninterrupted PC usage.	
	Automatic CPU throttling during scheduled scans	Automatic CPU throttling during scheduled scans in endpoints, so background scans will not affect endpoints' performance	
		Service Support	
Phone Support		For technical issue that need expert attention.	
Email Support		For technical issue that need expert attention.	

Regards

Internet & Network Security	Malware Protection	Antivirus or anti-virus software is software used to prevent, detect and remove malware, such as: computer viruses, malicious BHOs, hijackers, ransom ware, key loggers, backdoors, rootkits, trojan horses, worms, malicious LSPs, dialers, fraud tools, adware and spyware.	
	Phishing Protection	An anti-phishing service is a technological service that helps prevent unauthorized access to secure and/or sensitive information. Anti-phishing services protect various types of data in diverse ways across a variety of platforms.	
External Drives & Devices	Auto run Protection	Prevents External Drives against auto run malware infection	
	Scan External Drives	Scans external storage devices. Protects USB drives from auto run infections.	
Centralized Quarantine	Quarantine Files Management	The selected AV should quarantine a file keeps it on your machine but does not allow you to access it except through the virus program console. Usually the only reason to quarantine something is to wait and see if a new set of virus definitions can clean it and then let the program scan it again.	

Chat Support	The OEM should have Support Centre in India	
Remote Support	The vendor/OEM will give remote support	
Vision of Support	Need to ensure that every new update or feature upgrade or new feature/functions gets added to subscribers automatically. The subscribes doesn't have to wait for migration in the event of new feature addition/ feature upgrade.	
Additional Features		
MII	Completely made in India, including AV Engine & Web-server	
Security Information and Event Management (SIEM) Integration	Security information and event management (SIEM) support at no extra cost	

Regards