Notice Inviting Tender

Management Development Institute Gurgaon

Ref. No.: MDI/CC/2022-23/Antivirus/14 **Date:** Dec 23, 2022

Sub: Invitation of sealed quotations for 800 Nos of Licenses for End Point Security Antivirus Solution for a period of three years

Bid System	Single Bid
Last Date of Bid Submission	Dec 29, 2022, 11:00 AM
Bid should be addressed to	Senior Systems Analyst Computer Centre MANAGEMENT DEVELOPMENT INSTITUTE Mehrauli Road, Sukhrali Gurgaon - 122 007, Haryana (INDIA)

The Complete Tender details and any updates on the Tender will be available on the MDI Website at the link: https://mdi.ac.in/infrastructure/tenders.html

Checklist and Index of the Technical Bid Document in the Order indicated Below

S. No.	Document to be Attached	Whether Submitted
1.	Tender Document signed and stamped on each page	Yes ❑ / No ❑
2.	Filled in and signed Technical Bid on company's letter head	Yes ❑ / No ❑
3.	Profile of the Company	Yes ❑ / No ❑
4.	Client Details for Supplying & Installing Antivirus Solution	Yes ❑ / No ❑
5.	Authorized Distributor Certificate	Yes ❑ / No ❑
6.	Confirmation that Technical specifications are as per Annexure-1. Attach details of additional features offered	Yes ❑ / No ❑
8.	PAN, TAN, GST along with the copy of registration	Yes ❑ / No ❑
9.	Bank Account number with IFSC code, Bank name and Branch	Yes ❑ / No ❑

Terms & Conditions are as under:

1) The bid should be submitted on company letter head and should be submitted duly signed by the authorized person.
2) The financial bid shall be valid for at least 90 Days. Institute will not entertain any request in respect of escalation of price due to any reason whatsoever.
3) The items should be supplied and installed at MDI Campus, Gurgaon, nothing extra shall be paid towards the cartage, packing, forwarding, Octroi etc.
4) MDI reserve the right to accept or reject any or all the quotations without assigning any reason whatsoever.
5) In case the items are not delivered and installed within due date then penalty shall be imposed @ Rs. 1,000/- for each day subject to a maximum of Rs. 10,000/- (Rs. Ten thousand only).
6) MDI reserves the right to exclude any item or increase/decrease the number of items at the time of placing the order.
7) MDI reserves the right to allot/cancel the tenders invited as it may consider/deem fit and proper and to reject the tenders/applications without assigning any reasons at any stage.
8) No bid will be accepted on email. The bid must be submitted in hard copy in a sealed invoice superscribing "Bid for End Point Security Antivirus Solution for a period of three years"
9) **MDI may, at its discretion, extend the date for submission of the bid.**
10) **ACCEPTANCE AND WITHDRAWAL**

    The final acceptance of the tender would entirely vest with MDI, who reserves the right to accept or reject any tender, without assigning any reason whatsoever. There is no obligation on the part of MDI to communicate in any way with rejected bidders. After acceptance of the tender by MDI, the bidder shall have no right to withdraw his tender or claim higher price.
11) Bids received with incomplete information is liable for rejection.
12) Any Bid received by MDI after the deadline for submission of bids will be summarily rejected.
13) Any dispute/ difference arising out or relating to this Tender: Matters regarding any dispute shall be referred for arbitration to any Officer appointed by the Director of Management Development Institute Gurgaon, whose decision shall be binding and final.
14) Eligibility Criteria
    - The bidder should be a Company registered in India.
    - The bidder should have a good reputation in the market and their clientele shall preferably include reputed University/ Institute / PSU/ Govt. etc.

- The bidder should have appropriate support relationship as Distributor/Service provider etc. and must submit authorized distributor certificate documents.
- The bidder should have executed at least three similar work order of same or higher value during the last three years.

15) Evaluation Procedure and Selection of Bidder

- The work would be awarded to the L1 Tender.
- **Bid Rejection Criteria:** The bid shall conform generally to the specifications and terms and conditions given in this document. Notwithstanding the general conformity of the bids to the stipulated specifications, the following requirements will have to be particularly met by the Bidders without which the same will be considered as non-responsive and rejected
  - ✓ Non submission of signed &+ stamped tender documents on each and every page
  - ✓ Submission of unsigned financial bid.
  - ✓ Not submitting Authorized Distributor Certificate for the product quoted
  - ✓ Bid(s) not complying with Delivery, installation & commissioning, warranty, penalty, etc clauses will be rejected.
  - ✓ The bidder should quote for all the items mentioned in the tender, failing which, their offer will be rejected.
  - ✓ The bidder should have an office in Delhi NCR manned with their own qualified support staff/Engineer with their Customer Care Number

16) PAYMENT TERMS:

- 85% (Eighty Five percent) of the total bill value of items supplied will be paid within 1 month of complete delivery of Software Licenses, installation etc.
- 5% will be paid at the end of each year (First Year, Second Year and Third Year)

Date : (Signature)

Name of Vendor

Format-1

Sealed Quotation for delivery and installation of Digital Standby

<table>
<tr><th>S. No.</th><th>Description</th><th>Company Response</th><th>Remarks</th></tr>
<tr><td rowspan="4">1.</td><td>Profile of your firm/company</td><td>Yes □ / No □</td><td></td></tr>
<tr><td>Year of establishment</td><td></td><td></td></tr>
<tr><td>Number of employees</td><td></td><td></td></tr>
<tr><td>Annual Turnover and Profit for the last 3 Years.</td><td><table><tr><th>Year</th><th>1</th><th>2</th><th>3</th></tr><tr><td><b>Turnover</b></td><td></td><td></td><td></td></tr></table></td><td></td></tr>
<tr><td>2</td><td>Names &amp; addresses of prestigious clients of reputed Institute/ University/ PSU/ Govt etc. (at least three)</td><td>Yes □ / No □
<b>1.</b>
<b>2.</b>
<b>3.</b></td><td></td></tr>
<tr><td>3</td><td>Whether Authorized Distributor of the product quoted.
(Attached valid authorization Certificate)</td><td>Yes □ / No □</td><td></td></tr>
<tr><td>5</td><td>Contact details of the authorized person of the company.
1. Name :
2. Office Tel No.:
3. Mobile no. :
4. Official E-mail id:</td><td>Yes □ / No □</td><td></td></tr>
<tr><td>6</td><td>Whether blacklisted by any Company / Organization.</td><td>Yes □ / No □</td><td></td></tr>
<tr><td>7</td><td><b>The Items quoted meets the technical specifications as given in Annexure-1</b></td><td>Yes □ / No □</td><td></td></tr>
<tr><td>9</td><td>The product is quoted with 3 Year licenses.</td><td>Yes □ / No □</td><td></td></tr>
<tr><td>10.</td><td><b>Payment Terms :</b>
• 85% (Eighty Five percent) of the total bill value of items supplied will be paid within 1 month of complete delivery of Software Licenses, installation etc.
• 5% will be paid at the end of each year (First Year, Second Year and Third Year)</td><td>Yes □ / No □</td><td></td></tr>
<tr><td>11.</td><td><b>Delivery Time</b></td><td>Immediate (Please mention the time period required)
---</td><td></td></tr>
</table>

Format-2

Details of Clients for delivery and installation of Digital Standee (Insert Additional Rows to give Additional Client details)

S. No.	**Client Name** **(Institute / University/ PSU/ Govt.)**	**Product supplied (Name, Version etc)**	**Qty supplied**	**Client Contact No.**	**Client Email ID**	**PO Attached**
						Yes ❑ / No ❑
						Yes ❑ / No ❑
						Yes ❑ / No ❑

Annexure-1

Technical Specifications for 01 nos. of Digital Standee

***Attach technical data sheet of all the products quoted**

S. No.	Detailed Specifications of the Digital Standee System including the following	Compliance Attach separate sheet indicating deviations (if any)
1.	800 Nos of Licenses for End Point Security Antivirus Solution (End point Detection and Response) functionality for both Endpoints (Laptops / Desktops) and Servers (Windows/Linux) for a period of three years (Trend Micro/ McAfee/ Sophos/ Microsoft/ Symantec)	Yes ❑ / No ❑
	The solution must support up to 800 endpoints/clients	Yes ❑ / No ❑
	Solution must have a central console for defining policy, creating groups of systems/users, logging, deploying updates, reporting	Yes ❑ / No ❑
	Ability to exclude files and folders from scans. (Example: Exemptions for specific database folders)	Yes ❑ / No ❑
	Ability to completely stop the antivirus/EPP during application installs	Yes ❑ / No ❑
	Granular control of policy based on group/device/user	Yes ❑ / No ❑
	The solution should be able to perform push operations to endpoint clients	Yes ❑ / No ❑
	Console access should support using 3rd party systems authentication	Yes ❑ / No ❑
	Solution must use provide modern and easy remote deployment/ installation/ uninstallation methods (including script support)	Yes ❑ / No ❑
	Supported OS like Windows, Linux	Yes ❑ / No ❑
	Solution should be aligned and supported to the latest OS releases.	Yes ❑ / No ❑
	This solution will allow deploying the client and protecting machines running on terminal servers.	Yes ❑ / No ❑
	Agent must be lightweight. Present evidence of average CPU, memory and disk use during different activities with the capabilities below enabled	Yes ❑ / No ❑
	Solution is configurable for minimal system resource utilization	Yes ❑ / No ❑
	All files written on the file-system will monitored and statically analyzed. If found as potentially malicious the files will be emulated by sandboxing and quarantined if found as malicious	Yes ❑ / No ❑

	The solution must be able to completely clean the endpoint from any leftovers of the attack in the case the sandbox found the file to be malicious	Yes □ / No □
	The solution will detect and prevent exploitation techniques of trusted software.	Yes □ / No □
	The solution has the capability of blocking against the new RDP RCE attacks on unpatched systems.	Yes □ / No □
	Solution will automatically create an incident analysis for every detection/prevention that occurs. This analysis should include process execution trees even across boots if relevant.	Yes □ / No □
	Forensic report will automatically identify the malicious activity entry point and highlight the potential damage, remediation action and the entire chain of attack.	Yes □ / No □
	The Forensics report will log, present and un-obfuscate PowerShell scripts used during an attack.	Yes □ / No □
	The solution will be able to follow indirect methods of execution used by malware like WMI calls and Injections to be able to trace the activity of more advanced malware.	Yes □ / No □
	The solution must include the following sensors: Remote Execution Service Creation Process Discovery Application Window Discovery Scheduled Task Screen Capture Input Capture DDE (Dynamic Data Exchange)	Yes □ / No □
	Solution will allow for the searching of multiple type of undetected sensor data including File, Process, Network, Registry, Injection and User data.	Yes □ / No □
	The solution will allow for remediation of any file or process found through the EDR platform.	Yes □ / No □
	The solution will provide multiple manual remediation options, such as Quarantine, Kill Process and Forensics Analysis with remediation.	Yes □ / No □
	The solution will provide a central management ability to isolate machines remotely.	Yes □ / No □
	The solution must have the ability to view MAC addresses for every computer sending data.	Yes □ / No □
	The solution should generate periodic reports on malware types, types of vulnerabilities exploited etc.	Yes □ / No □
	Solution must provide agent health status	Yes □ / No □
	The solution should showcase affected process, affected registry keys & affected files in OS environment	Yes □ / No □

	The solution will be used to restrict or allow IPV6 network traffic.	Yes ❑ / No ❑
	The solution’s client Firewall should remain active during a client upgrade	Yes ❑ / No ❑
	The solution must include an option for Host Isolation to isolate or allow a specific host (access to network) that is under malware attack and poses a risk of propagation.	Yes ❑ / No ❑
	The solution will be used to restrict network access for specified applications. The Endpoint Security administrator defines policies and rules that allow, block or terminate applications and processes	Yes ❑ / No ❑
	The solution will be able to Whitelist\Blacklist applications	Yes ❑ / No ❑
	The solution will be used to restrict network access for specified applications. The Endpoint Security administrator defines policies and rules that allow, block or terminate applications and processes	Yes ❑ / No ❑
	The solution will be able to Whitelist\Blacklist applications	Yes ❑ / No ❑
	The solution will protect the computer from all kinds of malware threats, ranging from worms and Trojans to adware and keystroke loggers. The solution will centrally manage the detection and treatment of malware on the endpoint computers.	Yes ❑ / No ❑
	The solution will leverage multiple sensors to effectively and uniquely identify generic malware behaviours as well as malware family specific behaviours	Yes ❑ / No ❑
	The solution will immediately prevent or detect on malicious behaviours regardless if the machine is online or offline	Yes ❑ / No ❑
	The solution will detect and prevent file less attacks based on scripting.	Yes ❑ / No ❑
	The solution should protect against the "Pass The Hash" technique for credential theft.	Yes ❑ / No ❑
	The solution should detect malicious LNK (Windows Shortcut) files.	Yes ❑ / No ❑
	The solution should detect zero-day local privilege escalation (LPE).	Yes ❑ / No ❑
	The solution will integrate with Microsoft’s Anti-Malware Scan Interface (AMSI) to receive and analyse decoded scripts.	Yes ❑ / No ❑
	The solution must lock the user from using files until they are checked and found to be benign	Yes ❑ / No ❑
	The solution’s Static Detection Engine must monitor the access to files	Yes ❑ / No ❑
	The solution must be able to identify zero-days files even if they are not familiar with any reputation service	Yes ❑ / No ❑

	The solution will identify and block out-going communication to malicious C&C sites.	Yes ❑ / No ❑
	Support for Browsers like Chrome, Firefox, Safari, etc.	Yes ❑ / No ❑
	The solution must have scrubbing capabilities with no added hardware. Incoming files will be extracted of all potential malicious content such as scripts, macros and active content	Yes ❑ / No ❑
	When scrubbing, the original file must be accessible by end user if is found to be benign by the sandbox	Yes ❑ / No ❑
	Incoming files will be emulated by sandboxing for potentially malicious content.	Yes ❑ / No ❑
	The solution must block the user from browsing to a known malicious URLs or domains	Yes ❑ / No ❑
	The solution must provide URL filtering based on categories with additional Black/White listing	Yes ❑ / No ❑
	The solution must enforce "Safe Searching" feature when they employ the Google, Bing, Yahoo or any other search engines	Yes ❑ / No ❑
	Solution must use provide modern and easy remote deployment/installation/uninstallation methods (including script support)	Yes ❑ / No ❑
	Solution must capture detailed metadata around binaries and processes that are executed on endpoints. Details must include, but not limited to, the binary's hash (MD5, SHA256), publisher information, code signing details, frequency observed in our environment, version information, and filesystem owner	Yes ❑ / No ❑
	The solution should have the ability to control the level of messages to show to users	Yes ❑ / No ❑
	Solution must provide a way to isolate a system that ensures preventative controls are preserved through reboots. Isolation settings must be pre-set to allow endpoint to be isolated from threats but able to connect to investigation/remediation systems	Yes ❑ / No ❑
	Solution must be able to immediately apply preventive controls (block specific activity or known malicious, etc.)	Yes ❑ / No ❑
	The solution will allow custom user message notifications when connecting a device based on the scenario.	Yes ❑ / No ❑
	The solution will enforce endpoint computers to comply with security rules that are defined for the organization. Computers that do not comply will be shown as noncompliant and can apply restrictive policies to them.	Yes ❑ / No ❑
	The solution will enforce required Applications and Files based on the compliance settings by monitoring for the presence of specified files, registry values, and processes	Yes ❑ / No ❑

	that must be running or present on endpoint computers.	
	The solution will enforce prohibited Applications and Files based on the compliance settings by monitoring for the presence of specified files, registry values, and processes that are prohibited to be running or present on endpoint computers	Yes □ / No □
	The solution will enforce an Anti-Malware check to verify that computers have an anti-malware program installed and updated.	Yes □ / No □
	The solution will enforce Firewall rules to allow or block network traffic to endpoint computers based on connection information, such as IP addresses, ports, and protocols.	Yes □ / No □
	The solution will be used to determine if users can connect to wireless networks while on your organization's LAN to protect the network from threats associated with wireless networks.	Yes □ / No □
	The solution will define if users can connect to the organization network from hotspots in public places, such as hotels or airports.	Yes □ / No □

FORMAT-3

Financial Bid

Sealed Quotation for supply and installation of 01 nos. of Digital Stand

Sr. No.	**Description of Item & Specification(Model no if any)**	**Product Quoted**	**Qty. in Units**	**Unit Price in Rs.**	**Total Price excluding GST in Rs.**
1.	800 Nos of Licenses for End Point Security Antivirus Solution for a period of three years		800		
2.	Installation etc.				
3.	Total				
4.	GST				
5.	**Grand Total**				

Total Price in Figures: Rs.____
Total Price in Words: Rupees ____
Delivery Time: ____
Installation & Commissioning Time: ____

- **Delivery Mode:** Delivery at MDI Gurgaon, at site only
- Total bid price should be inclusive of all taxes and levies, transport, loading, unloading, installation and commissioning etc.
- **Warranty Period:** 3 years
- Delivery: Immediate.
- Installation Period: Immediately on delivery
- Quotation Validity Date: 90 days from the last date of Submission of quotation/tender.

Sign of bidder:- ____________________________
Name of bidder: - ____________________________
Firm's Name: ____________________________

Date: