INVITATION TO TENDER

AND

INSTRUCTIONS TO TENDERERS

FOR THE SUPPLY OF CENTRALIZED ANTIVIRUS SERVER SOLUTION ON CLOUD WITH ENDPOINT CLIENT AGENTS

Tender Ref. No: NABFINS/007/2026-27

NABFINS LIMITED, Bengaluru

TABLE OF CONTENTS

Sl. No.	Particulars	Page No.
1	Invitation to Tender and instructions to Tenderers	3 - 5
2	Disclaimer	6
3	Tender Notification	7
4	Instructions with regard to submission of Tender	8 - 13
5	Specifications (Annexure I)	14 - 18
6	Technical Bid Format (Annexure II)	19 - 22
7	Acceptance Certificate (Annexure III)	23
8	Organizational / Financial Profile of the Vendor/Bidder (Annexure IV)	24 - 25
9	Bidders Eligibility Criteria (Annexure V)	26
10	Specimen of Letter of Undertaking (Annexure VI)	27
11	Integrity pact (Annexure VII)	28 - 31
12	Bidder’s declaration on Land border (Annexure VIII)	32
13	OEM’s declaration on Land border (Annexure IX)	33
14	Checklist (Annexure X)	34
15	Financial Bid format (Annexure XI)	35

NABFINS LIMITED

FOR THE SUPPLY OF CENTRALIZED ANTIVIRUS SERVER SOLUTION WITH ENDPOINT CLIENT AGENT

NABFINS Limited Invites Tenders from the vendors for the supply of centralized antivirus server solution with endpoint client agent as per specifications given in the schedules (Annexure I) attached to the Tender form annexed hereto. The details of the Tender are given below

1	Bid Document Availability	Bid document can be downloaded from Company's website www.nabfins.org from 02nd November, 2026 till 4.30 pm on 23rd November, 2026
2	Pre-bid meeting	12th November, 2026 at 11:00 AM
3	Pre Queries	Last date of acceptance of Pre-bid queries 10th November, 2026 till 04:30 PM Pre-bid queries need to be sent to following email IDs To: nikesh.v@nabfins.org, & itsupport@nabfins.org
3	Last date for submission of Tender	23rd November, 2026 till 4:30 PM
4	Date and time of opening of Tender	Opening of Technical bid – 24th November, 2026 at 11:00 AM. Opening of Financial bid – will be communicated to Bidders who qualify the technical bid.
5	Address for Communication and submission of Tender	Chief Technology Officer NABFINS Limited, 3072, 14th cross, Banashankari , K R Road, Bengaluru – 560 070
6	Name and telephone number of the contact person	Mr. Nikesh Venugopal, **Mob:** 8861233112, **e-mail:** Nikesh.v@nabfins.org
7	Earnest Money Deposit	EMD shall be accepted by way of bank deposit only. EMD amount of ₹7,00,000/- (Rupees Seven Lakhs only) shall be deposited by the way of remittance to NABFINS Limited account (details mentioned below). The UTR of the transaction and screenshot should be indicated in the technical bid document. *All MSEs having registration as per provisions of the Public Procurement Policy for Micro and Small Enterprises i.e. District Industries Centre (DIC) or Khadi and Village Industries Commission (KVIC) or Khadi and Industries Board (KVIB) or Coir Board or National Small Industries Commission (NSIC) or directorate of

		Handicrafts and Handlooms or Udyog Aadhaar Memorandum or any other body specified by Ministry of MSME and Start-ups (recognised by DIPP) are exempted from submission of EMD only. Relevant certificates should be submitted by the bidder in this regard to avail exemption. Bank Account details: Acct no.: 32635856611 IFSC Code: SBIN0003286 Branch: SBI Jayanagar II Block branch The EMD of unsuccessful bidders will be returned without any interest whatsoever within 30 days of awarding of the contract. The EMD of the successful bidder shall be retained as performance security. The same shall be returned without any interest whatsoever within 30 days from the date of supply, configuration, and installation of end point security in all equipment (laptops, desktops & servers). *Tender without EMD will be rejected
8	Specification of Centralized antivirus server solution with endpoint client agents	Annexure I
19	Documents to be submitted	Tender documents shall be submitted in two cover bid mode. **Envelop 'A' Technical Bid: (Need to write "Technical Bid" on the envelop)** a) Technical bid as per Annexure II b) Brochure provided by OEM c) MAF from OEM d) Acceptance Certificate as per Annexure III e) EMD - Details of bank transfer f) Organizational / Financial Profile of the Vendor/Bidder as per Annexure IV with Certificate from CA g) Bidders Eligibility Criteria as per Annexure V h) Undertaking by the Authorized Signatory of the Vendor/Bidder as per Annexure VI i) Integrity pact as per Annexure VII j) Self-Declaration Certificate for Land Border Annexure VIII k) Declaration certificate for Land Boarder from OEM Annexure IX l) Checklist X

		Envelop 'B' Financial Bid: (Need to write "Financial Bid" on the envelop) m) Financial bids as per Annexure XI "Technical bid" and "Financial bid", both the Envelopes are to be sealed in Master Envelope. Bidder should write "Tender for Antivirus Solution 2026-27" on the Master envelope
10	Validity of price quotation	NABFINS LIMITED will be executing contract with the selected vendor for 03 years. The price quoted will be valid for 03 years from the date of execution of contract. The price for the end point licenses will be on pro-rate basis.

DISCLAIMER

The information contained in this Tender document or information provided subsequently to Bidder(s) or applicants whether verbally or in documentary form/email by or on behalf of NABFINS Limited (Company), is subject to the terms and conditions set out in this Tender document and all other terms and conditions subject to which such information is provided.

This Tender document is neither an agreement nor an offer and is only an invitation by the Company to the interested parties for submission of bids. The purpose of this Tender is to provide the Bidder(s) with information to assist the formulation of their proposals. This Tender does not claim to contain all the information each Bidder may require. Each Bidder should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information in this Tender and where necessary obtain independent advices / clarifications.

The Company may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this Tender. No contractual obligation whatsoever shall arise from the Tender process until a formal contract is signed and executed by duly authorized officers of the Company with the selected Bidder.

The Company, its employees and advisors make no representation or warranty and shall have no liability to any person, including any applicant or Bidder under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this Tender or otherwise, including the accuracy, adequacy, correctness, completeness or reliability of the Tender and any assessment, assumption, statement or information contained therein or deemed to form part of this Tender or arising in any way for participation in this Bid stage.

The Company also accepts no liability of any nature whether resulting from negligence or otherwise, howsoever caused arising from reliance of any Bidder upon the statements contained in this Tender.

The issue of this Tender does not imply that the Company is bound to select a Bidder and the Company reserves the right to reject all or any of the Bidders or Bids without assigning any reason whatsoever.

The Bidder shall bear all its costs associated with or relating to the preparation and submission of its Bid including but not limited to preparation, copying, postage, delivery, fees, expenses associated with any demonstrations or presentations which may be required by the Company or any other costs incurred in connection with or relating to its Bid. All such costs and expenses will remain with the Bidder and the Company shall not be liable in any manner whatsoever for the same or for any other costs or other expenses incurred by a Bidder in preparation for submission of the Bid, regardless of the conduct or outcome of the Bidding process.

TENDER NOTIFICATION

NABFINS Limited

Bengaluru

Ref .No.: NABFINS/007/2026-27
Date: 02-11-2026

TENDER NOTICE

Sealed bids are invited from the vendors/suppliers for the supply of centralized antivirus server solution with endpoint client agents.

Information relating to the Tender can be viewed and the Tender documents can be downloaded from our website www.nabfins.org.

The sealed Tenders should reach the undersigned on or before **23th November, 2026 till 4:30 PM**

Sd/-

Chief Technology Officer

INSTRUCTIONS WITH REGARD TO SUBMISSION OF TENDER

1. BIDDER QUALIFICATIONS

Offers are invited only from those Vendors/Bidders who fulfil the following eligibility criteria:

a) The bidder should be a company registered in India under the relevant acts, such as the Companies Act 2013, or a partnership registered under the Indian Partnership Act 1932, or a partnership firm registered under the Limited Liability Partnership Act 2008, with its registered office in India - Copy of Certificate of Incorporation/GST Registration and PAN Card to be submitted along with technical bid.

b) The bidder should have experience of a minimum of 5 years in providing IT/IT services – Self declaration certificate in letter head need to be submitted.

a) The product offered should comply with the specifications indicated in detailed specifications of the endpoint security. The bidder should submit supporting documents along with the Technical Offer.

b) The bidder should be direct channel partner of the OEM and should be the one-point contact for the entire project.

c) The selected vendor need to provide 04 nos. of resource for the installation of end points solution in all the IT assets used by NABFINS LIMITED. Installation at branch offices need to be done remotely with the help of remote desktop software.

d) The bidder should provide the Manufacturer's Authorised partner certificate. The Authorised partner certificate should not be older than 02 financial years preceding the financial year in which the Tender / quotation is being submitted. Offers without proper Authorised partner certificate shall be treated as incomplete and shall be rejected.

e) The Vendor/Bidder should not have been blacklisted by any Central/State Government Organization or PSU for any corrupt and fraudulent practice. An Undertaking by the Authorized Signatory on the letter head of the Vendor/Bidder should be submitted as a part of Technical Offer (Annexure VI).

f) The vendor/bidder should be a profit making entity for the past 3 (three) years and its Annual Turnover during each of the last 3 years should not be less than Rs.300 lakhs. This should be individual Company's turn over and net profit and not that of group of companies. Certificate issued by company's CA stating the profit and turnover for past 3 years should be provided as part of Technical offer. (not balance sheet or P&L)

g) The Vendor/Bidder should mandatorily furnish pre-contract integrity pact, as per Annexure VII. The Vendor/Bidder has to submit the same duly signed on a non-judicial stamp paper of Rs.200/- at the time of submission of the Tender document.

h) All bidders regardless of whether they share land border with India are required to mandatorily submit Self Declaration Certificate in respect of self as well as OEMs whose product they are offering as per the format given in Annexure VIII & IX. Any bidder/OEM from a country which shares a land border with India will be eligible to bid in this Tender only if the bidder/OEM is registered with the Competent Authority (i.e. Registration Committee constituted by Department for Promotion of Industry and Internal Trade (DPIIT)).

2. Earnest Money Deposit (EMD):

EMD shall be accepted by way of bank deposit only. EMD amount of ₹7,00,000/- (Rupees Seven Lakhs only) shall be deposited by the way of remittance to NABFINS Limited account (details mentioned below). The UTR of the transaction and screenshot should be indicated in the technical bid document. *All MSEs having registration as per provisions of the Public Procurement Policy for Micro and Small Enterprises i.e. District Industries Centre (DIC) or Khadi and Village Industries

Commission (KVIC) or Khadi and Industries Board (KVIB) or Coir Board or National Small Industries Commission (NSIC) or directorate of Handicrafts and Handlooms or Udyog Aadhaar Memorandum or any other body specified by Ministry of MSME and Start-ups (recognised by DIPP) are exempted from submission of EMD only. Relevant certificates should be submitted by the bidder in this regard to avail exemption.

Bank Account details:

Acct no.: 32635856611
IFSC Code: SBIN0003286
Branch: SBI Jayanagar Il Block branch

The EMD of unsuccessful bidders will be returned without any interest whatsoever within 30 days of awarding of the contract.

The EMD of the successful bidder shall be retained as performance security. The same shall be returned without any interest whatsoever within 30 days from the date of supply of Endpoint client agents with license, configuration of Centralized antivirus server solution on cloud and after completion of end point security agents in laptops, desktops and servers by the resource aligned by the vendor/bidder.

Tender without EMD will be rejected. The EMD should form part of the Technical Bid Document submitted by the Vendor/Bidder. Failure to comply with this condition viz., Bid Security of Rs.7,00,000/-(Rupees Seven Lakhs only) shall result in summary rejection of the Quotation/Bid.

The EMD shall be forfeited if

1) The Vendor/Bidder withdraws his offer during the period of validity of the bid.
2) The Vendor/Bidder does not fulfil the contract obligations.

Agreement:

The issue of Purchase Order by NABFINS LIMITED shall be construed as a binding contract. NABFINS will be executing a contract with the selected bidder with 03 years validity for the supply of end point licenses. The cost for the end point licenses shall remain same during the contract period. The validity of all end point licenses shall expire on same day after 03 years of contract. The cost of end point licenses purchased during the contract period shall be calculated on pro-rata basis.

Confidentiality:

The details of the proposed purchase shall be treated as confidential information between NABFINS LIMITED and Vendor/Bidder. Any such information shall not be passed on in part or in full to any third party without NABFINS LIMITED's prior written approval.

The Bidder/Vendor shall ensure that complete confidentiality is maintained by them and all their personnel, with regard to all information relating to NABFINS LIMITED. Unless required under law, Bidder/Vendor assures NABFINS LIMITED that neither Bidder/Vendor nor any of their personnel shall at any time divulge, disclose or make known to any third parties any business process or date, trust, accounts, matters or transactions whatsoever pertaining to NABFINS LIMITED.

Order cancellation:

NABFINS LIMITED reserves its right to cancel the entire/unexecuted part of the Purchase Order at any time by assigning appropriate reasons in the event of one or more of the following conditions: -

a) Delay in supply of endpoint licenses and configuration of centralised console beyond three weeks from the date of acceptance/receipt of the work order/Purchase Order (except with written permission from NABFINS LIMITED).
b) Any other appropriate reason incidental to clause (a) above.

Right to Accept or Reject the Bid

NABFINS LIMITED shall reserve the right to accept/ reject and cancel the bid, amend the quantity under any lot or withdraw any lot at any stage before or after acceptance of bid/ issue of acceptance letter/ sale order/ delivery order/ deposit of the full sale value by the bidder, without assigning any reason therefor and the value of such material, if paid for, shall be refundable. NABFINS LIMITED shall not be responsible for damage/ loss to bidders on account of such withdrawal at any stage from the sale.

Force Majeure

a) The parties shall not be liable for default or non-performance of the obligations under the contract, if such default or non-performance of the obligations under this contract is caused by Force Majeure.
b) For the purpose of this clause, "Force Majeure" shall mean an event beyond the control of the parties, due to or as a result of or caused by acts of God, wars, insurrections, riots, earthquake and fire, events not foreseeable but does not include any fault or negligence or carelessness on the part of the parties, resulting in such a situation.
c) In the event of any such intervening Force Majeure, each party shall notify the other party in writing of such circumstances and the cause thereof immediately within five calendar days. Unless otherwise directed by the other party, the party pleading Force Majeure shall continue to perform/render/discharge other obligations as far as they can reasonably be attended/fulfilled and shall seek all reasonable alternative means for performance affected by the Event of Force Majeure.

d) In such a case, the time for performance shall be extended by a period(s) not less than the duration of such delay. If the duration of delay continues beyond a period of three months, the parties shall hold consultations with each other in an endeavour to find a solution to the problem.

e) Notwithstanding above, the decision of NABFINS LIMITED shall be final and binding on the Bidder.

3. BID PRICE:

a) The prices should be quoted in Indian Rupees only.
b) All duties, taxes and other levies payable by the vendor shall be included in the total price. The cost of insurance, packing, forwarding, if any, shall be borne by the bidder
c) NABFINS may issue single purchase order for full quantity or multiple purchase orders as and when required. The total quantity indicated in Annexure I is indicative only. NABFINS may issue purchase order for additional number of licenses over and above what is mentioned in Annexure I during the validity period.
d) Corrections, if any, shall be made by crossing out, initialling, and re-writing.
e) The rates quoted by the bidder shall be valid for 3 years. NABFINS LIMITED will execute contract with the selected vendor for the supply of endpoint licenses. During the contract period the price remains same and will be calculated on pro-rata basis.
f) The bidder must consider the cost for 04 nos. of resources for the installation of end point security in all the PCs/Laptops/servers as mentioned in requirement (Annexure 1).
g) Each bidder shall submit only one quotation. If more than one bid is submitted, all the bids submitted by the bidder shall be rejected.
h) Price bids shall be signed by the person authorized by the Vendor/Bidder.

4. AWARD OF CONTRACT:

The purchaser will award the contract to the bidder based on Quality and Cost-Based Selection (QCBS)

Proposals will finally be ranked according to their combined technical (ST) and financial (SF) scores as follows:

S = (ST x Tw) + (SF x Fw)

Where S is the combined score, and Tw and Fw are weights assigned to Technical Proposal and Financial Proposal that shall be 0.70 and 0.30, respectively.

ST is the technical score of the bidder and SF in the commercial score of the bidder on the basis of commercials submitted.

Formula for calculating SF and ST are as follows:

SF = (Lowest Commercial Figure/ Bidder's Commercial Figure) * 100

ST = (Technical Score of the bidder/ Highest Technical Score) * 100

The selected Bidder/Vendor having the highest combined score in the aforesaid manner, shall be treated as the first ranked Bidder/Vendor. NABFINS may also maintain a reserve list of Bidders/Vendors, which may be used in case the first ranked Bidder/Vendor withdraws or fails to comply with the requirements as the case may be.

Note:

The highest technical bidder shall not automatically qualify for becoming selected bidder and for award of contract by NABFINS.

The Successful bidder shall be the first ranked bidder (having the highest combined score). The final decision on the successful bidder will be taken by NABFINS.

If for some reason, the successful bidder fails to execute an agreement within a specified timeline, NABFINS reserves the right to award the contract to the next most eligible bidder based on the final evaluation scope of technical evaluation scores and commercial prices quoted.

In case of a tie of Total Score between two or more bidders, the Bid with higher technical score would be chosen as the successful Bidder.

NABFINS will calculate the scores up to two decimal points only. If the third decimal point is greater than .005 the same shall be scaled up else, it shall be scaled down to arrive at two decimal points.

5. Right to Acceptance:

The Company does not bind itself to accept the lowest on any Tender and reserves the right of accepting the whole or any part of the Tender or portion of the quantity offered, wherever applicable, and the bidder shall supply the same at the rate quoted.
The bidder, whose bid is accepted, will be notified for the award of contract by the purchaser prior to expiry of the quotation validity period. The terms of the accepted offer shall be incorporated in the purchase order.

6. DELIVERY:

The centralized antivirus server solution with endpoint client agent with the mentioned quantity shall be delivered within three weeks from the date of issue of Purchase Order and complete the installation of end point security agents in all the PCs, Laptops, & servers within 60 days from the delivery of licenses.

7. PENALTY:

1. In the event of a delay in the delivery of licenses and configuration of the centralized console beyond three (03) weeks from the agreed schedule, a penalty of 0.2% of the total quoted cost shall be deducted from the final payment for each additional week of delay.
2. In the event of delay in installation of end point security in equipment (PCs, Laptops, & servers) beyond sixty (60) days a penalty of 0.2% of the total quoted cost shall be deducted from the final payment for each additional week of delay.

8. TERMS OF PAYMENT:

Payment shall be made by the Company

1. **First Installment – 50% of the Quoted Price:**
   50% of the total quoted price shall be released upon successful delivery of the entire quantity of licenses specified in the Work Order/Purchase Order and completion of the configuration of the centralized management console, as detailed in Annexure-I.
2. **Second Installment – Remaining 50% of the Quoted Price:**
   The balance 50% of the total quoted price shall be released upon successful completion of the installation of endpoint licenses on all PCs, laptops, and servers covered under the Work Order/Purchase Order, along with submission of the installation report to the Company.
3. **Bank Account Details:**
   The successful bidder shall provide the necessary bank account details, including the account holder's name, bank name, branch, account number, and IFSC code, for processing and remittance of payments.

9. DELIVERY OF TENDER:

Both technical bid and financial bid to be placed in envelope. The Envelope must be super scribed with "Tender for Antivirus Solution 2026-27" along with Tender reference number.

The sealed Tender should be addressed to:

Chief Technology Officer
NABFINS Limited
3072, 14th cross, K R Road
Bengaluru - 560 070

Bids in sealed covers should reach the above address latest by 13th November, 2026 till 4:30 PM Tenders submitted after the specified time shall not be considered and no intimation will be sent in this regard.

The Company reserves the Right to reject any Tender which fails to comply with the above instructions. All Tenders should be sent by Post or through messenger, to drop the Tender in the sealed Tender box provided in the office. It is the responsibility of the Tenderer to see that his/her Tender offer is delivered by the specified time at the above address. All further communication should be addressed to the officer named above and by title only.

Sd/-
Chief Technology Officer

Annexure I

Background:

This solution is for Servers, Laptops, and Desktops, used by NABFINS LIMITED at Head Office and branch offices which is located in 19 states. Solution must provide centralized protection, monitoring, detection, investigation, and response for endpoints including desktops, laptops, servers, and supported virtual machines.

The bidder shall provide an enterprise-grade endpoint security/Endpoint Detection and Response (EDR) solution from a reputed and globally recognized cybersecurity manufacturer, with proven deployments in enterprise/government organizations. The solution shall provide centralized management, next-generation antivirus/anti-malware, behavioral detection, ransomware protection, EDR capabilities, vulnerability/exposure visibility, web and application control, and real-time threat monitoring.

Scope of Work for selected vendor/bidder:

1. Configure the centralized console on cloud and provide access to NABFINS IT department.
2. Configure / apply rules in the console as per the requirement of NABFINS.
3. Supply required quantity of end point licenses as per the work order / Purchase order.
4. Allocate 04 nos. of resource (man power) for the installation of end point security in all nodes (Laptops, Desktops & Servers) of NABFINS.
5. The allocated resources need to uninstall the existing end point security from the laptops/desktops/servers and install new end point security.
6. The resources allocated by the vendor need to perform the Installation at branch office PCs remotely with the help of remote desktop software.
7. The resource need to coordinate with branch offices and take remote of desktop/laptop and install the end point solution.
8. The said 04 nos. of resource must be available at NABFINS Head office, Bangalore for the installation of end point security during the office hours until completion of installation of end point security in all desktops, Laptops & servers.

Scope of Work for selected OEM:

1. The End point security OEM need extend support to SIEM tool provider for integration. The integration shall happen during the contract period.
2. The console must be hosted on cloud having DC and DR inside the country.

Specifications and required quantity for Centralized antivirus server solution with endpoint client agents:

Centralized Antivirus Server Solution (Console)	:	1 No.
End Point Client Agents for laptops &desktops	:	2339 Nos.
End Point Client Agents for Windows Servers	:	15 Nos.

Sl. No.	Area	Minimum Technical Requirement
1	Scope	Solution shall provide centralized protection, monitoring, detection, investigation, and response for endpoints including desktops, laptops, servers, and virtual machines.
2	Supported OS	Windows 10/11, Windows Server 2025 STD, Windows Server 2019 STD, Linux and mac OS versions must be supported by the OEM.
3	Endpoint Protection	Real-time protection against viruses, worms, Trojans, spyware, ransomware, rootkits, fileless malware, exploits, and other known/unknown threats.
4	Malware Detection	Signature-based, heuristic, behavioral, machine-learning/AI-based and reputation-based detection mechanisms.
5	Ransomware Protection	Dedicated ransomware protection with behavioral detection, exploit prevention, and protection against unauthorized encryption/modification of files.
6	Exploit Protection	Protection against exploitation of OS, application, browser and memory vulnerabilities, including zero-day attack techniques.
7	Web Protection	URL/web reputation filtering, malicious website blocking, phishing protection, and protection against drive-by downloads.
8	Application Control	Ability to control/block unauthorized, malicious or potentially unwanted applications. Allow listing/deny listing capabilities shall be available.
9	Device Control	Control of removable media such as USB storage devices, external drives and other peripherals. Policies shall support allow/block/read-only controls where applicable.
10	Firewall	Host-based firewall with centralized policy management and ability to define inbound/outbound application, port and network rules.
11	Behavioural Monitoring	Continuous monitoring of endpoint processes, memory, files, registry, scripts, network connections and other relevant activities for suspicious behaviour.
12	EDR Capability	Solution shall provide Endpoint Detection and Response capabilities, including endpoint telemetry, threat hunting, investigation, incident timeline and response actions.
13	Incident Response	Administrators shall be able to remotely isolate/quarantine an infected endpoint, terminate malicious processes, quarantine files and initiate remediation from the central console.
14	Central Management	Web-based centralized management console for deployment, configuration, monitoring, alerting, reporting and policy management.

15	Policy Management	Role-based policies shall be configurable based on endpoint group, department, location, operating system or other organizational criteria.
16	Automatic Updates	Automatic updates for malware signatures, detection engines, threat intelligence and security components without requiring manual intervention.
17	Threat Intelligence	Integration with continuously updated threat intelligence/reputation services for identification of malicious files, URLs, IP addresses and domains.
18	SIEM Integration	Solution shall support integration with existing SIEM/SOC platforms using standard mechanisms such as Syslog, API, CEF/LEEF or equivalent.
19	Vulnerability Management	Solution should identify vulnerable applications/OS components and provide risk-based visibility of endpoint vulnerabilities.
20	Security Alerts	Real-time alerts for malware detection, ransomware activity, suspicious behavior, policy violations, exploit attempts and other critical security events.
21	Dashboard & Reports	Central dashboard providing endpoint health, protection status, detected threats, incidents, vulnerabilities, policy compliance and security trends.
22	Audit Logs	Comprehensive and tamper-resistant logs of administrator activities, endpoint events, policy changes, detections and response actions.
23	Identity & Access	Role-Based Access Control (RBAC), configurable administrative roles and support for integration with enterprise directory/identity services. MFA support should be available for administrative access.
24	Data Security	Communication between endpoint agents and management infrastructure shall be encrypted using industry-standard secure protocols.
25	Agent Security	Endpoint agent shall have self-protection/tamper protection to prevent unauthorized disabling, modification or uninstallation.
26	Performance	Agent shall have minimal impact on endpoint CPU, memory, disk and network resources during normal operation. Vendor shall specify resource requirements and performance impact.
27	Offline Protection	Endpoint protection shall continue to function when the endpoint is temporarily disconnected from the management server/network.
28	Cloud	Solution shall be cloud-hosted, as specified by the purchaser. Vendor shall clearly state architecture, data location and infrastructure requirements.

29	Scalability	Solution shall support the complete number of endpoints specified in the tender and provide scalability for future endpoint expansion without major architectural changes.
30	High Availability	Management infrastructure shall support high availability, redundancy and backup/restore mechanisms appropriate for enterprise deployment.
31	Deployment	Solution shall support centralized/remote deployment using enterprise software-distribution mechanisms and/or directory services.
32	Licensing	License shall cover all specified endpoint devices for the complete contract period, including security updates, threat intelligence and software upgrades.
33	API	REST/API or equivalent interfaces should be available for integration with SOC, SIEM, SOAR, ITSM and other enterprise security tools.
34	Compliance	The proposed solution shall comply with applicable information-security, data-protection and regulatory requirements / Statutory requirements of the country.
35	OEM Support	OEM/manufacturer support shall be available throughout the contract period, including security updates, patches and technical assistance.
36	SLA	Vendor shall provide defined support SLA for critical, high, medium and low severity incidents, including escalation mechanism and OEM involvement.
37	Warranty/Updates	All software updates, patches, new detection capabilities and product upgrades released during the subscription/license period shall be provided without additional license cost.
38	Training	Vendor shall provide administrator training and operational documentation for deployment, policy configuration, monitoring, incident investigation and response.
39	Documentation	Complete installation, configuration, administration, troubleshooting and API documentation shall be provided.
40	Technical presentation	Eligible bidders need to provide a demonstration.
41	XDR	Extended Detection & Response across endpoint, identity, email, network and cloud telemetry
42	Endpoint DLP	Detect/prevent sensitive-data leakage through USB, web upload, cloud storage, email, printing, clipboard etc.
43	MITRE ATT&CK	Map detections/incidents to MITRE ATT&CK tactics and techniques
44	IOC Management	NABFINS shall have the capability to create, update, manage, search, and enforce custom Indicators of Compromise (IOCs) for blocking and detection. The solution shall support custom IOCs including file hashes, IP addresses, domains, URLs, and other supported indicators.

45	Automated Response	Automated response/playbooks based on defined conditions
46	Endpoint Asset Inventory	Hardware, OS, software, user, IP, agent and security-status inventory
47	Software Inventory	Centralized inventory of installed applications and versions
48	EOL/EOS Detection	Identify unsupported/EOL operating systems and applications
49	Patch Visibility	Identify missing security patches and provide remediation recommendations
50	Endpoint Risk Score	Risk score based on vulnerabilities, threats, configuration and endpoint posture
51	Security Posture	Dashboard showing agent health, protection status, policy compliance and security posture
52	PowerShell/Script Monitoring	Detection and monitoring of PowerShell, WMI, scripts and LOLBins
53	Credential Attack Detection	Detection of credential dumping, LSASS access and similar credential attacks
54	DLP Reporting	Centralized DLP incidents, evidence, users, endpoints and policy-violation reports
55	DLP Policy Modes	Monitor, alert, block and quarantine modes
56	Cloud Storage Control	Control uploads to unauthorized/personal cloud storage
57	Web Upload Control	Detect/block sensitive-file uploads through browsers
58	SIEM Bi-directional Integration	Event export plus response/action integration where supported
59	ITSM Integration	Automatic incident/ticket creation and status updates

Annexure II

Technical bid format:

The bidder need to confirm that the below mentioned features and facilities are available in proposed product (Yes/No):

Sl. No.	Area	Minimum Technical Requirement	Yes/No
1	Scope	Solution shall provide centralized protection, monitoring, detection, investigation, and response for endpoints including desktops, laptops, servers, and virtual machines.	
2	Supported OS	Windows 10/11, Windows Server 2025 STD, Windows Server 2019 STD, Linux and mac OS versions must be supported by the OEM.	
3	Endpoint Protection	Real-time protection against viruses, worms, Trojans, spyware, ransomware, rootkits, fileless malware, exploits, and other known/unknown threats.	
4	Malware Detection	Signature-based, heuristic, behavioral, machine-learning/AI-based and reputation-based detection mechanisms.	
5	Ransomware Protection	Dedicated ransomware protection with behavioral detection, exploit prevention, and protection against unauthorized encryption/modification of files.	
6	Exploit Protection	Protection against exploitation of OS, application, browser and memory vulnerabilities, including zero-day attack techniques.	
7	Web Protection	URL/web reputation filtering, malicious website blocking, phishing protection, and protection against drive-by downloads.	
8	Application Control	Ability to control/block unauthorized, malicious or potentially unwanted applications. Allow listing/deny listing capabilities shall be available.	
9	Device Control	Control of removable media such as USB storage devices, external drives and other peripherals. Policies shall support allow/block/read-only controls where applicable.	
10	Firewall	Host-based firewall with centralized policy management and ability to define inbound/outbound application, port and network rules.	
11	Behavioural Monitoring	Continuous monitoring of endpoint processes, memory, files, registry, scripts, network connections and other relevant activities for suspicious behaviour.	
12	EDR Capability	Solution shall provide Endpoint Detection and Response capabilities, including endpoint telemetry, threat hunting, investigation, incident timeline and response actions.	
13	Incident Response	Administrators shall be able to remotely isolate/quarantine an infected endpoint, terminate malicious processes, quarantine files and initiate remediation from the central console.	

14	Central Management	Web-based centralized management console for deployment, configuration, monitoring, alerting, reporting and policy management.	
15	Policy Management	Role-based policies shall be configurable based on endpoint group, department, location, operating system or other organizational criteria.	
16	Automatic Updates	Automatic updates for malware signatures, detection engines, threat intelligence and security components without requiring manual intervention.	
17	Threat Intelligence	Integration with continuously updated threat intelligence/reputation services for identification of malicious files, URLs, IP addresses and domains.	
18	SIEM Integration	Solution shall support integration with existing SIEM/SOC platforms using standard mechanisms such as Syslog, API, CEF/LEEF or equivalent.	
19	Vulnerability Management	Solution should identify vulnerable applications/OS components and provide risk-based visibility of endpoint vulnerabilities.	
20	Security Alerts	Real-time alerts for malware detection, ransomware activity, suspicious behavior, policy violations, exploit attempts and other critical security events.	
21	Dashboard & Reports	Central dashboard providing endpoint health, protection status, detected threats, incidents, vulnerabilities, policy compliance and security trends.	
22	Audit Logs	Comprehensive and tamper-resistant logs of administrator activities, endpoint events, policy changes, detections and response actions.	
23	Identity & Access	Role-Based Access Control (RBAC), configurable administrative roles and support for integration with enterprise directory/identity services. MFA support should be available for administrative access.	
24	Data Security	Communication between endpoint agents and management infrastructure shall be encrypted using industry-standard secure protocols.	
25	Agent Security	Endpoint agent shall have self-protection/tamper protection to prevent unauthorized disabling, modification or uninstallation.	
26	Performance	Agent shall have minimal impact on endpoint CPU, memory, disk and network resources during normal operation. Vendor shall specify resource requirements and performance impact.	
27	Offline Protection	Endpoint protection shall continue to function when the endpoint is temporarily disconnected from the management server/network.	

28	Cloud	Solution shall be cloud-hosted, as specified by the purchaser. Vendor shall clearly state architecture, data location and infrastructure requirements.	
29	Scalability	Solution shall support the complete number of endpoints specified in the tender and provide scalability for future endpoint expansion without major architectural changes.	
30	High Availability	Management infrastructure shall support high availability, redundancy and backup/restore mechanisms appropriate for enterprise deployment.	
31	Deployment	Solution shall support centralized/remote deployment using enterprise software-distribution mechanisms and/or directory services.	
32	Licensing	License shall cover all specified endpoint devices for the complete contract period, including security updates, threat intelligence and software upgrades.	
33	API	REST/API or equivalent interfaces should be available for integration with SOC, SIEM, SOAR, ITSM and other enterprise security tools.	
34	Compliance	The proposed solution shall comply with applicable information-security, data-protection and regulatory requirements / Statutory requirements of the country.	
35	OEM Support	OEM/manufacturer support shall be available throughout the contract period, including security updates, patches and technical assistance.	
36	SLA	Vendor shall provide defined support SLA for critical, high, medium and low severity incidents, including escalation mechanism and OEM involvement.	
37	Warranty/Updates	All software updates, patches, new detection capabilities and product upgrades released during the subscription/license period shall be provided without additional license cost.	
38	Training	Vendor shall provide administrator training and operational documentation for deployment, policy configuration, monitoring, incident investigation and response.	
39	Documentation	Complete installation, configuration, administration, troubleshooting and API documentation shall be provided.	
40	Technical presentation	Eligible bidders need to provide a demonstration.	
41	XDR	Extended Detection & Response across endpoint, identity, email, network and cloud telemetry	
42	Endpoint DLP	Detect/prevent sensitive-data leakage through USB, web upload, cloud storage, email, printing, clipboard etc.	
43	MITRE ATT&CK	Map detections/incidents to MITRE ATT&CK tactics and techniques	

44	IOC Management	NABFINS shall have the capability to create, update, manage, search, and enforce custom Indicators of Compromise (IOCs) for blocking and detection. The solution shall support custom IOCs including file hashes, IP addresses, domains, URLs, and other supported indicators.	
45	Automated Response	Automated response/playbooks based on defined conditions	
46	Endpoint Asset Inventory	Hardware, OS, software, user, IP, agent and security-status inventory	
47	Software Inventory	Centralized inventory of installed applications and versions	
48	EOL/EOS Detection	Identify unsupported/EOL operating systems and applications	
49	Patch Visibility	Identify missing security patches and provide remediation recommendations	
50	Endpoint Risk Score	Risk score based on vulnerabilities, threats, configuration and endpoint posture	
51	Security Posture	Dashboard showing agent health, protection status, policy compliance and security posture	
52	PowerShell/Script Monitoring	Detection and monitoring of PowerShell, WMI, scripts and LOLBins	
53	Credential Attack Detection	Detection of credential dumping, LSASS access and similar credential attacks	
54	DLP Reporting	Centralized DLP incidents, evidence, users, endpoints and policy-violation reports	
55	DLP Policy Modes	Monitor, alert, block and quarantine modes	
56	Cloud Storage Control	Control uploads to unauthorized/personal cloud storage	
57	Web Upload Control	Detect/block sensitive-file uploads through browsers	
58	SIEM Bi-directional Integration	Event export plus response/action integration where supported	
59	ITSM Integration	Automatic incident/ticket creation and status updates	

Signature of authorised person: Place:

Full Name:

Date: Seal:

Annexure III
Acceptance Certificate

1. I/ We, _____Son / Daughter /Wife of _____ Proprietor / Director / authorized signatory of the agency / Firm, mentioned above, is competent to sign this declaration and execute this Tender document;

2. I have carefully read and understood all the terms and conditions of the Tender and undertake to abide by them;

3. I do hereby certify that the rates of each items have been quoted in the Financial Bid.

4. The information / documents furnished along with the above application are true and authentic to the best of my knowledge and belief. I/We, am/ are well aware of the fact that furnishing of any false information / fabricated document would lead to rejection of Tender at any stage.

5. I, do hereby certify that our firm has neither been blacklisted by any of the Govt. Organization / Public Sector / Pvt. Limited Company, etc. with which the firm had contracted for supply of IT infrastructure or software during the last three years nor has been penalised by such Offices/organizations for supply of poor/spurious materials etc.

6. The supply of items / services will be done as per the specification mentioned in the Tender form.

Signature of authorised person

Full Name:

Date:

Place:

Seal:

Annexure IV

Organizational / Financial Profile of the Vendor/Bidder

1	Constitution: *(Tick one)*	Proprietary/Partnership/Private Ltd. /Public Ltd.
2	Established since:	
3	Address for Communication:	
4	Classification: *(Tick one)*	Solution provider/ System Integrator/Hardware vendor/ Bidder/ Software Developer
5	If Joint Venture, then specify names of Partners in the Service Support Co, JV	
6	Others *(please specify)*	(Position and Designation)
7	Name(s) of Proprietor(s) / Partner(s) / Directors (s)	
8	Number of Hardware/System Software Engineers familiar with the Product offered	

9	Total Number of Employees	
10	Number of locations where Service Support Centres are available for catering to the products being offered.	
11	Products: (*details*)	
12	Business Figures for 3years (Certificate from CA indicating 3 years (2023-24, 2024-25, 2025-26) annual turnover and profit) to be attached:	

Year	Turnover (Rs. Lakh)	Net Profit (Rs. Lakh)
2025-26		
2024-25		
2023-24		

Signature of Vendor/Bidder
Name:

Annexure V

Bidders Eligibility Criteria

Sl. No.	Eligibility Criteria	Details of Eligibility	Supporting Document
1	Turnover of the Company- The bidder must have minimum - RS.300 Lakh turnover in each financial year.	2025-26-Rs. _____ Lakhs 2024-25-Rs. _____ Lakhs 2023-24-Rs. _____ Lakhs	Certificate from CA indicating the turnover and profit year-wise.*
2	Company should have earned profits in the last 3 Financial Years, viz.	2025-26-Rs. _____ Lakhs 2024-25-Rs. _____ Lakhs 2023-24-Rs. _____ Lakhs	
3	Escalation Matrix indicating Contact Person, Telephone Number, Email details of L1, L2 and L3 support Managers of the bidder.	L1 Name: Contact Number: Email: L2 Name: Contact Number: Email: L3 Name: Contact Number: Email:	
4	Escalation Matrix indicating Contact Person, Telephone Number, Email details of L1, L2 and L3 support Managers of the OEM.	L1 Name: Contact Number: Email: L2 Name: Contact Number: Email: L3 Name: Contact Number: Email:	

*The document certified by Chartered Accounts should mandatorily contain Unique Document Identification Number.

Annexure VI

FORMAT OF UNDERTAKING, TO BE FURNISHED ON COMPANY LETTER HEAD WITH REGARD TO BLACKLISTING/ NON- DEBARMENT, BY ORGANISATION

UNDERTAKING REGARDING BLACKLISTING / NON – DEBARMENT

To,

NABFINS LIMITED,
#3072, 14th Cross, K. R. Road,
Banashankari 2nd Stage,
Bengaluru – 560 070,
Karnataka, India

We hereby confirm and declare that we, M/s ----------, is not blacklisted/ De-registered/ debarred by any Government department/ Public Sector Undertaking/ Private Sector/ or any other agency for which we have Executed/ Undertaken the works/ Supply/Services.

For ----------

Authorised Signatory

Date:

Annexure VII

(Print on Rs. 200/- stamp paper)

INTEGRITY PACT
Between
NABFINS LIMITED
hereinafter referred to as "The Principal"
And
..... hereinafter referred to as "The Bidder/Contractor"

Preamble

The principal intends to award, under laid down organizational procedures, contract/s for the supply of End point security licenses with centralised console. The principal values full compliance with all relevant laws of the land, rules, regulation, and economic use of resources and of fairness/transparency in its relations with its Bidder(s) and/or Contractor(s).
In order to achieve these goals, the Principal will appoint Independent External Monitor(IEM) who will monitor the tender process and the execution of the contract for compliance with the principles mentioned above.

Section 1 -Commitments of the Principal

(1) The Principal commits itself to take all measures necessary to prevent corruption
and to observe the following principles: -

a) No employee of the Principal, personally or through family members, will in connection with the tender for, or the execution of a contract, demand, take a promise for or accept, for serf or third person, any material or immaterial benefit which the person is not legally entitled to.
b) The Principal will, during the tender process treat all Bidder(s) with equity and reason. The Principal will, in particular, before and during the tender process, provide to all Bidder(s) the same information and will not provide to any Bidder(s) confidential / additional information through which the Bidder(s) could obtain an advantage in relation to the tender process or the contract execution.
c) The Principal will exclude from the process all known prejudiced persons.

(2) If the Principal obtains information on the conduct of any of its employees which is a criminal offence under the IPC/PC Act, or if there be a substantive suspicion in this regard, the Principal will inform the Chief Vigilance Officer and in addition can initiate disciplinary actions.

Section 2 -Commitments of the Bidder(s)/Contractor(s)

(1) The Bidder(s) / Contractor(s) commit themselves to take all measures necessary to prevent corruption. The Bidder(s) / Contractor(s) commit themselves to observe the following principles during participation in the tender process and during the contract execution:

a) The Bidder(s) / Contractor(s) will not, directly or through any other person or firm, offer, promise or give to any of the Principal's employees involved in the tender process or the execution of the contract or to any third person any material or other benefit which he/she is not legally entitled to, in order to obtain in exchange any advantage of any kind whatsoever during the tender process or during the execution of the contract.
b) The Bidder(s)/Contractor(s) will not enter with other Bidders into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications, certifications, subsidiary's, contracts, submission or non-submission of bids or

any other actions to restrict competitiveness or to introduce cartelisation in the bidding process.

c) The Bidder(s)/Contractor(s) will not commit any offence under the relevant IPC/PC Act; further the Bidder(s) / Contractor(s) will not use improperly, for purposes of competition or personal gain, or pass on to others, any information or document provided by the Principal as part of the business relationship, regarding plans, technical proposals and business details, including information contained or transmitted electronically.

d) The Bidder(s)/Contractor(s) of foreign origin shall disclose the name and address of the Agents/representatives in India, if any. Similarly, the Bidder(s)/Contractors(s) of Indian Nationality shall furnish the name and address of the foreign principals, if any.

e) The Bidder(s) /Contractor(s) will, when presenting their bid, disclose any and all payments made, is committed to or intends to make to agents, brokers or any other intermediaries in connection with the award of the contract.

f) Bidder(s) Contractor(s) who have signed the Integrity Pact shall not approach the Courts while representing the matter to IEMs and shall wait for their decision in the matter.

(2) The Bidder(s) /Contractor(s) will not instigate third persons to commit offences outlined above or be an accessory to such offences.

Section 3 - Disqualification from tender process and exclusion from future contracts

If the Bidder(s) /Contractor(s), before award or during execution has committed a transgression through a violation of Section 2, above or in any other form which put their reliability or credibility in question, the Principal is entitled to disqualify the Bidder(s) / Contractor(s) from the tender process.

Section 4 - Compensation for Damages

(1) If the Principal has disqualified the Bidder(s) from the tender process prior to the award according to Section 3, the Principal is entitled to demand and recover the damages equivalent to Earnest Money Deposit/Bid Security.

(2) If the Principal has terminated the contract according to Section 3, or if the Principal is entitled to terminate the contract according to Section 3, the Principal Shall be entitled to demand and recover from the Contractor liquidated damages of the Contract value or the amount equivalent to Performance Bank Guarantee.

Section 5 - Previous transgression

(1) The Bidder declares that no previous transgressions occurred in the last three years with any other Company in any country conforming to the anti-corruption approach or with any Public Sector Enterprise in India that could justify his exclusion from the tender process.

(2) If the Bidder makes incorrect statement on this subject, he can be disqualified from the tender process.

Section 6 - Equal treatment of all Bidders / Contractors/ Subcontractors

(1) In case of Sub-contracting, the Principal Contractor shall take the responsibility of the adoption of Integrity Pact by the Sub-contractor.

(2) The Principal will enter into agreements with identical conditions as this one with all Bidders and Contractors

(3) The Principal will disqualify from the tender process all bidders who do not sign the Pact or violate its provisions.

Section 7 - Criminal charges against violating Bidders(s) / Contractor(s)/ Subcontractor(s)

If the Principal obtains knowledge of conduct of a Bidder, Contractor or Subcontractor, or of an employee or a representative or an associate of a Bidder, Contractor or Subcontractor which constitutes corruption, or if the Principal has substantive suspicion in this regard, the Principal will inform the same to the Chief Vigilance Officer.

Section 8 - Independent External Monitor

(1) The Principal appoints competent and credible Independent External Monitor for this Pact after approval by the Central Vigilance Commission of NABARD. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this agreement.

The Independent External Monitor appointed for NABFINS LIMITED is
Shri Otem Dai, IAS (Retd)
Gute Gomro, C-Sector,
Papun Pare District,
Itanagar 791111,
jinachal Pradesh
Email Id: otemdai@hotmail.com

(2) The Monitor is not subject to instructions by the representatives of the parties and
Performs his/her functions neutrally and independently. The Monitor would have access to all Contract documents, whenever required. It will be obligatory for him / her to treat the information and documents of the Bidders /Contractors as confidential. He / she reports to the Chairman, NABARD.

(3) The Bidder(s)/Contractor(s) accepts that the Monitor has the right to access without restriction to all Project documentation of the Principal including that provided by the Contractor. The Contractor will also grant the Monitor, upon his/her request and demonstration of a valid interest, unrestricted and unconditional access to their project documentation. The same is applicable to Sub-contractors.

(4) The monitor is under contractual obligation to treat the information and documents of the Bidder(s) /Contractor(s) / Sub-contractor(s) with confidentiality. The Monitor has also signed declarations on `Non-disclosure of Confidential Information and of `Absence of Conflict of Interest'. In case of any conflict of interest arising at a later date, the IEM shall inform Chairman, NABARD and recuse himself/herself from that case.

(5) The Principal will provide to the Monitor sufficient information about all meetings among the parties related to the Project, provided such meetings could have an impact on the contractual relations between the Principal and the Contractor. The parties offer to the` Monitor the option to participate in such meetings.

(6) As soon as the Monitor notices, or believes to notice, a violation of this agreement, he/she will so inform the Management of the Principal and request the Management to discontinue or take corrective action, or to take other relevant action. The monitor can in this regard submit non-binding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action.

(7) The monitor will submit a written report to the Chairman, NABARD within 8 to 10 weeks from the date of reference or intimation to him by the Principal and, should the occasion arise, submit proposal for correcting problematic situations.
(8) If the Monitor has reported to the Chairman, NABARD, a substantiated suspicion of an offence under the relevant IPC/PC Act, and the Chairman NABARD has not, within reasonable time, taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.
(9) The word 'Monitor' would include both singular and plural.

Section 9 - Pact Duration

This Pact begins when both parties have legally signed it. It expires for the Contractor 12 months after the last payment under the contract, and for all other Bidders 6 months after the contract has been awarded. Any violation of the same would entail disqualification of the bidders and exclusion from future business dealings.
If any claim is made/lodged during this time, the same shall be binding and continue to be valid despite the lapse of this pact as specified above, unless it is discharge / determined by the Chairman of NABARD.

Section 10 - Other provisions

(1) This agreement is subject of Indian Law, Place of performance and jurisdiction is the Head Office of the Principal, i.e. Mumbai.
(2) Changes and supplements as well as termination notices need to be made in writing. Side agreements have not been made.
(3) If the Contractor is a partnership or a consortium, this agreement must be signed by all partners or consortium members.
(4) Should one or several provisions of this agreement turn out to be invalid, the remainder of this agreement remains valid. In this case, the parties will strive to come to an agreement to their original intentions.
(5) Issues like Warranty/Guarantee etc. shall be outside the purview of IEMs.
(6) In the event of any contradiction between the Integrity Pact and its annexure, if any, the Clause in the Integrity Pact will prevail.

(For & On behalf of the principal)	(For & on behalf of the Bidder/Contractor)
(Office seal)	(Office seal)

Place:

Date:

Witness 1:
(Name & Address)

Witness 2:
(Name & Address)

Annexure VIII

SELF DECLARATION CERTIFICATE

(To be furnished by bidder in their respective letter heads)

I have read the office memorandum F. No. 6/18/2019-PPD dated: 23-07-2020, issued by Ministry of Finance, Department of Expenditure, Public Procurement Division Inserting Rule 144(xi) in GFRs 2017 which defines clauses regarding restriction on procurement from a bidder of a Country which shares a land border with India. I certify that this bidder is not from such a country or, if from such a country, has been registered with the competent authority, I certify that this bidder fulfils all requirements in this regard and is eligible to be considered.

(Where bidder whose products are being offered is from a country sharing land border with India, evidence of valid registration by the Competent Authority shall be attached mandatorily)

Sl. No.	Bidder Name	Is bidder from a country which shares a land border with India? (Yes/No) (If yes, please attach the evidence of valid registration)

Signature of authorised person

Full Name:

Date:

Place:

Seal:

Annexure IX

SELF DECLARATION CERTIFICATE

(To be furnished by OEM in their respective letter heads)

I have read the office memorandum F. No. 6/18/2019-PPD dated: 23-07-2020, issued by Ministry of Finance, Department of Expenditure, Public Procurement Division Inserting Rule 144(xi) in GFRs 2017 which defines clauses regarding restriction on procurement from a bidder of a Country which shares a land border with India. I certify that this OEM is not from such a country or, if from such a country, has been registered with the competent authority, I certify that this OEM fulfils all requirements in this regard and is eligible to be considered.

(Where OEM whose products are being offered is from a country sharing land border with India, evidence of valid registration by the Competent Authority shall be attached mandatorily)

Sl. No.	OEM Name	Is OEM from a country which shares a land border with India? (Yes/No) (If yes, please attach the evidence of valid registration)

Signature of authorised person

Full Name:

Date:

Place:

Seal:

Annexure X
CHECKLIST TO BE ATTACHED WITH THE TENDER

Sl. No.	Documents	Yes/No
1	Copy of Certificate of Incorporation/GST Registration and PAN Card	
2	Self-Declaration Certificate on the Company Letterhead Confirming a Minimum of Five Years of Experience in Providing IT/IT Services.	
3	Technical bid as per Annexure II	
4	Brochure provided by OEM	
5	MAF from OEM	
6	Acceptance Certificate as per Annexure III	
7	EMD - Details of bank transfer	
8	Organizational / Financial Profile of the Vendor/Bidder as per Annexure IV with Certificate from CA	
9	Bidders Eligibility Criteria as per Annexure V	
10	Undertaking by the Authorized Signatory of the Vendor/Bidder as per Annexure VI	
11	Integrity pact as per Annexure VII	
12	Self-Declaration Certificate for Land Border as per Annexure VIII	
13	Declaration certificate for Land Boarder from OEM as per Annexure IX	
14	Financial Bid as per Annexure XI	

Important Notice: An incomplete offer bid may be summarily rejected. In order to aid the bidders in submitting the bid, a checklist is included in the bid Document. The bidders must duly fill this and submit along with the technical bid.

Annexure XI

FINANCIAL BID FOR THE SUPPLY OF CENTRALIZED ANTIVIRUS SERVER SOLUTION ON CLOUD WITH ENDPOINT CLIENT AGENTS

Tender Ref. No: NABFINS/007/2026-27

Name of Vendor / Bidder: ……..

Sl. No.	Description	Qty. (Nos)	Unit Price excluding GST (Rs.)	Total excluding GST (Rs.)	GST (Rs.)	Total including GST (Rs.)
A	**B**	**C**	**D**	**E=(C X D)**	**F**	**G=(E+F)**
1	Centralized Antivirus Server Solution (Console)	1				
2	End Point Client Agents for laptops & desktops	2339				
3	End Point Client Agents for Windows Servers	15				
4	Cost for resource (man power) for installation of endpoint security	4				
Grand Total:						
Net Amount in words:						

I/we have understood & agree to the terms and conditions of contract as mentioned in Tender (Ref: NABFINS/007/2026-27)

Date: _____

Place: _____

Stamp & Signature of Bidder