



MADHYA PRADESH FOREST DEPARTMENT



Invites Tender for Supply of
**Antivirus Endpoint Detection and Response
(EDR) for network security.**

OFFICE OF PRINCIPAL CHIEF CONSERVATOR OF FORESTS

(Information Technology)

Second floor, "C" block, Van Bhawan, Tulsi Nagar, Link Road No 2 Bhopal-462003.(MP)

Phone no. 0755 – 2524302, 2674302, email: -apccfit@mp.gov.in

Website: <https://www.mpforest.gov.in>





OFFICE OF PRINCIPAL CHIEF CONSERVATOR OF FORESTS

Wing - Information Technology Van Bhawan, Bhopal, 462003

Email: apccfit@mp.gov.in, Ph. - 0755-2524302, 2674302

पत्र क्रमांक / सूची / MPFD_IT_2026_01_01

भोपाल, दिनांक 12/01/2026

::::: Notice Inviting Tender :::::

**Antivirus Endpoint Detection and Response(EDR)
for network security.**

"The Forest Department has invited online tenders/bids for the supply of Antivirus Endpoint Detection and Response(EDR)for network. Proposals must be submitted exclusively through the portal: www.mptenders.gov.in."

Important Dates

| | Date |
|---------------------------------|--------------------|
| 1 Online Publishing | 13-Jan-2026 |
| 2 Online Submission Start | 13-Jan-2026 |
| 3 Online Submission Ending | 29-Jan-2026 |
| 4 Opening of Technical Proposal | 30-Jan-2026 |

| | |
|-----------------------------|----------------|
| Tender Fee | Rs 2,000/- |
| Online EMD (Through Portal) | Rs. 1,00,000/- |

For Technical specifications, timelines and other relevant details, please refer to the document on the www.mptenders.gov.in portal including the Tender document. Please read all document carefully before submitting proposal & financial bid.

**ADDITIONAL PRINCIPAL CHIEF CONSERVATOR OF FORESTS
(Information Technology)
Forest Department, Van Bhawan, Bhopal (MP)**



1. Definitions

In this document, unless otherwise mentioned or expressed clearly, the terms 'Competent Authority', 'Tenderer', 'Bidder', 'Committee' and 'Supply of Equipment's' would have meaning as given below:

Competent Authority: Madhya Pradesh Forest Department Acting through: APCCF (IT), Forest Department, Bhopal, Madhya Pradesh or any person authorized by Madhya Pradesh Forest Department or abovementioned authority.

Tenderer or Bidder: The Firm/Company who buys the tender document, signs and submits the Tender / BID document and bids for the contract and/or awarded the Contract to implement Tender for 'Supply of EDR', as the reference may indicate; it shall also include associates, licenses, collaborators, and agents.

Committee: Committee means committee(s) constituted by Madhya Pradesh Forest Department acting through office of Principal Chief Conservator of Forests (Head Of Forest Force), in relation for the invitation of the BID and selection of the Competent Tenderer for the purpose of this BID Supply of EDR as per the Specifications specified in this document, for use in Madhya Pradesh Forest Department.

Maintenance: Maintenance of the EDR supplied by the Vendor/Tenderer will be for the period of Three Years, from the date of supply, in which the employees of the Bidder will be engaged for the maintenance/repair of the EDR.

Warranty: Warrantee of EDR and services for a **period of Three years** from the date of supply.

Purchaser: Purchaser means MP Forest Department acting through Addl. Principal Chief Conservator of Forest (IT) Madhya Pradesh, or any person authorized by Madhya Pradesh Forest Department.

Vendor/Supplier: Means the Tenderer/ Bidder who has been declared the successful tenderer (bidder) and has been offered to enter into the agreement with the purchaser and who has entered into the agreement to execute the work/provide goods and services within the scope of this tender.

Authorized Suppliers: Means the Tenderer/ Bidder, who wins the Technical Bid and then Financial Bid and is authorize to supply the EDR to the Madhya Pradesh Forest Department,

OEM: Means Original Equipment Manufacturer

BOQ: Means Bill of Quantity

F O R: Stands for Freight on Road.



2. General conditions:

1. E-offers prepared in accordance with the procedures enumerated in this document then should be submitted online on website <https://mptenders.gov.in> EMD is also to be submitted online in <https://mptenders.gov.in> .
2. The competent authority reserves to itself the right to invite the fresh Tenders or BID and to place orders against any quantity of any items in this Tender / BID without specifying any reasons.
3. Competent authority may cancel the tender and all proceedings relating thereto without assigning any reason.
4. Bidder are advised to study the Bid document carefully and thoroughly. Submission of Proposal shall be deemed to have been done after careful study and examination of the Bid document with full understanding of its implications.
5. Bidders are also advised to ascertain whether they meet the eligibility criteria for bidding for the same. Incomplete bids will not be accepted. Bid should quote for all the items mentioned in **Section-IV** on a single responsibility basis. Bids with partial response are liable to be rejected.
6. Bid with price variation clauses or with vague terms are liable to be ignored and rejected. Counter offers shall not be considered. Incomplete tenders are liable to be rejected.
7. This Tender is non-transferable. Assignment and subletting is not permitted. Information regarding associates and principals is to be disclosed in the tender technical bid itself.
8. Tender/Bid can also be downloaded from the website of Madhya Pradesh Forest Department <https://mpforest.gov.in> Bid will only be considered when submitted online with suitable tender fee at <https://mptenders.gov.in> website.
9. All formats and Forms should be duly filled up carefully after complete preparation of bid and uploaded correctly in <https://mptenders.gov.in> . If the bidder, who wants to enclose some other additional relevant document, can add such documents separately in concerning bid.
10. The support personnel must be capable to provide maintenance and support services Independent of principals for the period of 3 (Three) years
11. Once the selected bidder successfully completes the bidding process, He/She will be termed as the Authorized Supplier.
12. Companies or bidders should be in compliance with the criteria specified in the office memorandum F.No.6/18/2019-PPD dated 23-07-2020 of the public procurement division of the Ministry of Finance, Government of India.
13. Order for the purchase of equipment's will be placed by additional principal chief conservator of forests.

Addl. PRINCIPAL CHIEF CONSERVATOR OF FORESTS

(Information Technology)

Van Bhawan, Bhopal (MP)



3. PROJECT OBJECTIVE

The objective of this project is to deploy server hardware and virtual infrastructure (both) at the IT-Hub, and to configure and manage Endpoint Detection and Response (EDR) along with server security solutions to establish a robust, secure, and integrated IT infrastructure for 550 users of the Madhya Pradesh Forest Department.

The proposed infrastructure will support the Department's operational, data security, and software requirements—ensuring seamless performance, secure data management, and interoperability across all systems.

4. SCOPE OF WORK

The scope of work under this project shall include, but not be limited to, the following activities:

1. Supply and Installation of an Enterprise-grade EDR Antivirus Solution for all Departmental users.
2. Deployment of a Centralized Management Server at the Department's Head Office.
3. Integration of the deployed solution with the Department's existing IT infrastructure.
4. Training, Documentation, and Knowledge Transfer for designated departmental staff to ensure effective use and management of the solution.
5. Comprehensive Warranty and Technical Support for a minimum period of three (3) years from the date of successful commissioning.

5. ELIGIBILITY CRITERIA/ REQUIREMENTS

1. OEM or Authorized Partner of the proposed solution. In case of Authorized Partner, tender specific OEM MAF should be submitted at the time of bidding.
2. Successful execution of at least 2 similar projects in Government/PSU/large enterprises. Purchase Order/Work Order copies should be submitted for the same.
3. The bidder must have at least two certified engineers in the proposed EDR security software. OEM-issued certification proof must be submitted with the bid.
4. Valid GST, PAN, Incorporation or Gumashta certificates.
5. Average turnover of last 3 years 1Cr, CA Certified Turnover Certificate or Audited Balance sheet should be submitted at the time of bidding.
6. Proven experience in discovery of acknowledged vulnerabilities.
7. Possession of a range of security intelligence services to demonstrate strength in the cybersecurity domain.
8. Independent third-party test validation (AV-TEST, AV-Comparatives, SE Labs) proving high protection rates against ransomware and advanced threats.
9. Submit Annexure-2

6. EVALUATION CRITERIA

1. Technical Evaluation.
2. Financial Evaluation.

Note :- Only technically qualified bidders will be considered for financial evaluation.



7. EDR REQUIREMENTS DETAILS

1. Solution should support, malware detection, ML-based defense, firewall, cloud mode, ARP spoofing protection, HTTPS inspection, device differentiation, cloud integration, application controls, email scanning, IDS/IPS, Office 365 protection, etc.
2. Refer Annexure-1 For detailed technical specification. Bidder has to submit Technical Compliance for the same on Letter head, along with datasheet of the product.

8. VALIDITY OF THE TENDER / BID:

Offer should be kept open for acceptance for a period of 90 days from the date of submission of Tender Bid. A bid valid for a shorter period may be rejected by the purchaser as non-responsive. Any increase in rates within this period will not be entertained and will result in forfeiture of EMD and / or Security Deposit. In the absence of express indication of Tenderer's, it should be deemed that, they are willing to keep their offer open for acceptance for a further period of 90 days from the above stipulated above.

9. PROCEDURE FOR SUBMISSION OF PROPOSALS:

- 8.1 No bid will be considered, unless and until each page of the bid documents is duly signed in original by the authorized signatory. Prices should not be indicated in the Pre-qualification or Technical Bid. It will lead to rejection of bid. All the columns of the quotation form shall be duly, properly and exhaustively filled in. The rates and units shall not be overwritten. Rates shall be both in the figures and words. It is mandatory for all bidders to quote Freight on Road (F.O.R). destination given in (prices inclusive of all taxes like GST, excise duty, freight, octroi, insurance, customs and any other taxes what so ever etc.). No any change shall be entertained in duties after bid submission.
- 8.2 Financial Bids determined to be substantially responsive will be checked by the evaluation committee for any errors. If there is a discrepancy between the quoted rate in figures and the quoted rate in words, the rate in words will take precedence. Arithmetic errors will be rectified on the following basis:
 - (A) If there is a discrepancy between the unit rate and the total cost that is obtained by multiplying the unit rate and quantity, the unit rate multiplied by quantity shall prevail and the total cost will be corrected unless in the opinion of the evaluation committee there is an obvious placement of the decimal point in the unit rate, in which case the total cost as quoted will govern and the unit rate corrected.
 - (B) If there is a discrepancy between the total bid amount and the sum of various costs, the sum of the various costs shall prevail and the total bid amount will be corrected.
- 8.3 The sum of the amount stated in the Form of Financial Bid will be adjusted by the evaluation committee in accordance with the above-mentioned point for the correction of errors and, shall be considered as binding upon the bidder. If the bidder does not accept the corrected amount of bid, its bid will be rejected, and the EMD shall be forfeited. Any omission in filling the columns of "units" and "rate" or pertaining to the Taxes/levies, service tax as applicable etc., shall be deemed to be treated as inclusive in the total project cost. All corrections must be duly signed by the Bidder.



- 8.4 All the bid papers must be signed before uploading bid online. The information submitted must be definitive and specific. Vague terms, incomplete information, Counter offers, and 'uncalled for' correspondence shall not be entertained. The authorized signatory of the Bidder must sign each page and at the last page it must be clearly indicated that all the terms and conditions mentioned herein are acceptable to the Bidder unconditionally.
- 8.5 Bidder is required to submit the complete proposal along with annexures & brochures etc. The proposal has to be signed in original by the authorized representative of the Bidder. The proposal shall be exactly according to the presented formats given in the TENDER documents (RFP). All columns of the prescribed formats should be filled, and all questions in the tender document must be answered. Any additional information should be enclosed separately and referred to in the relevant column in the proposal formats. Modifications / rewording of formats shall not be acceptable. No column should be marked as "NIL" or "Zero", "0" etc. Where no price is proposed to be charged for any item or its parts required to be supplied, it should be clearly mentioned in so many words.
- 8.6 The Bidder is expected to examine carefully all instructions, forms, terms and specifications in the Tender document. Failure to furnish all information required in the Tender Document or submission of a proposal not substantially responsive to the Tender Document in every respect will be at the Bidders risk and shall result in rejection of the proposal.

10. LANGUAGE:

The proposal prepared by the Tenderer and all correspondences, documents relating to the proposals exchanged by the Tenderer and the Competent Authority, shall be written in English/Hindi language. Competent Authority may permit any Tenderer any printed literature or any document in any other language accompanied by authenticated English translation. For the purpose of interpretation only English translation shall be acceptable.

11. EARNEST MONEY DEPOSIT:

A sum of fixed amount should be deposit as EMD online through (<https://mptenders.gov.in/>). The Earnest money will not be refunded on any account what so ever until the Bid finalized and in the event of any firm backing out from their offer, the Earnest money is liable to be forfeited. No interest shall be claimed on EMD amount. Bid received without or with inadequate EMD shall be liable to be rejected.

The successful bidder shall furnish an Earnest Money Deposit (EMD) amounting to 3% of the awarded tender value, in the form of a Performance Bank Guarantee (PBG), Bank Demand Draft (DD), or Bank Fixed Deposit (FD), as acceptable to the tendering authority.

12. FINANCIAL BID DOCUMENTS:

Financial Bid with price in Indian National Rupees (INR) must be submitted in prescribed formats as online BOM.

13. WARRANTY/MAINTENANCE:

Tenderer shall provide Warranty and support of all the service and system for three years from the installation Period.

14. DELIVERY PERIOD:

- a) EDR delivered and Installation within 15 days from the date of intimation of acceptance of bid.
- b) The supply shall be carried out at the Head Office of the Madhya Pradesh Forest Department, and all costs related to delivery and execution shall be borne by the Bidder.



15. PROCEDURE OF FINALIZATION OF BIDS:

- a. Firstly, the pre-qualification bid shall be opened online. At the time of opening of PQ Document, the authorized representative may remain present. Committee may ask the bidder any additional document/ information if required, to form its opinion as qualification of the bidder. The technical bid of only bidders qualifying in pre- qualification stage shall be opened.
- b. The information submitted by the Bidders in the technical bid documents shall be tabulated and compared with specifications given in the tender form. It will thus be ascertained whether the product offered by the bidder matches with the specification of the purchaser as given in the technical specifications in this tender document.
- c. The committee would be entitled to call for any further information, document, undertaking and may also interview the authorized representative of the bidder in order to satisfy itself about the eligibility of the bidder, technical specifications of the EDR. The committee would be within its right to get any enquiry, secret or open conducted for the purpose. The information, documents submitted and undertaking given by the bidder or its authorized representative to the committee should be deemed to be the part of the "technical bid" of the bidder. The decision of the committee on technical suitability of the offer shall be final.
- d. Out of all the bidders, committee shall prepare a list of the eligible/qualified bidder whose product/solution satisfies the Technical specifications as given in this document and is overall acceptable to purchaser being satisfied with bidder's capacity to full fill the supplies terms within stipulated time.
- e. Financial bids of only qualified Tenderers shall be opened. Rest bids shall not be considered and such short-listed bidders will be intimated about the date and time accordingly. At the time of the opening of Financial Bids, authorized representatives may remain present. It shall not be obligatory to accept only the lowest financial bid.
- f. Bidders must understand that concerned committee and the competent authority may opt for any bid for the reason given for such preference. Technical qualification does not mean that all bids stands at equal footing in terms of quality, reliability, and use worthiness, ease of handling, recurring maintenance and operation cost, down time / up time expected life/service period after expiry of warranty period or often claimed life period etc. These may be among some of considerations on the basis of which concerned committee may recommend any item to be procured and competent authority may accept such item. While making such decisions, the committee(s) may rely on or call for user feedback from M.P. Forest Department employees or from any other Government organization or other user who is/has used the offered item in this past.

16. STANDARD OF PERFORMANCE:

The Tenderer shall carry out the supply order and carry out its obligations under the agreement with due diligence, efficiency, economy and techniques. The Tenderer shall also adhere to professional, engineering and consulting standards recognized by international professional bodies and shall observe sound management, technical and engineering practices. The Tenderer shall apply appropriate advanced technology and safe and effective equipment, machinery, material and methods. The Tenderer shall always act in respect of any matter relating to this agreement, as faithful advisors to the Competent Authority and shall always support and safeguard the legitimate interests of Competent Authority in any dealing with a third party.



17. ACCEPTANCE TESTING AND INSPECTION:

The Supply of EDR for Madhya Pradesh Forest Department will be tested by the Final Acceptance & Test Committee as per Acceptance Test Procedure (ATP) as formulated and approved by the Competent Authority or his nominee. At the time of testing etc. Representative of bidder may remain present.

18. RIGHT TO VARY QUANTITIES:

- 1) The Competent authority reserves the right to vary the quantity within 6 months of execution of agreement without any change in price or other items and conditions with commensurate increase or decrease in delivery period. The quantity indicated in the Notice Inviting Tender may vary. Tenderer shall be bound to supply the users in such a quantity as required by Madhya Pradesh Forest Department.
- 2) The competent authority also reserves the right to place part order on the selected vendor. It must be clearly understood that the demand may fluctuate and no definite quantity can be guaranteed. The essence of the contract is price per item for the contract period stipulated. The approximate requirements are given in the tender schedule / bill of material.
- 3) The competent authority will be entitled to have protection of the price fall to be extended to it.
- 4) The purchaser reserves to himself the right to invite the fresh Tenders and to place orders against any quantity of any items in this Tender without specifying any reasons.

19. CONSIDERATION – Price, Taxes etc. and Payment Terms:

Payment Milestone:

| S No. | Payment | Terms |
|--------------|--|---|
| 1 | 90% of the total value including taxes | Will be released on the delivery of all Items. |
| 2 | 10% of the total value including taxes | The remaining 10% of the total amount will be paid after compilation and installation certificate of all users of MPFD. |

- The Tenderer will be entitled to receive consideration after completion of the respective delivery and "Final Acceptance Test" of all the items to be supplied by the bidder at the places specified by the Madhya Pradesh Forest Department.
- The prices quoted for the items shall be firm throughout the period of agreement and shall not be subject to any upward modification whatsoever. The rates should be quoted F.O.R. at Madhya Pradesh Forest Department. The prices quoted shall be all inclusive.
- The Tenderer shall be entirely responsible for all taxes, duties, license fees etc. For completion of delivery.



20. PENALTY CLAUSE:

- If the supply of the material is not completed in the stipulated time as prescribed in this document:
- a) Penalty of 0.5% per week of the Project cost shall be imposed up to maximum of 5 weeks in case of delay beyond 5 weeks' contract will be terminate after receiving the penalty. The decision of APCCF-IT will be final.
 - b) To purchase else-where, without notice to the Tenderer on Tenderer's account and at the Tenderer's risk, the items not delivered or others of a similar description (where offers exactly complying with the particulars are not in opinion of the competent authority readily procurable, such opinion being final) without canceling the contract in respect of the consignment not yet due for delivery, and /or.
 - c) To cancel the contract or portion thereof and if so desired to purchase the items at the risk and cost of the Tenderer, and/or.
 - d) To forfeit the Security Deposit to the extent of the loss incurred by the Government. In the event of action being taken under (a), (b) and (c) above, the Tenderer shall be liable for any loss, which the Government may sustain on that account but the Tenderer shall not be entitled to any gain on purchase made against default.
 - e) Penalty may be deducted from amount payable to vendor.

21. TERMINATION FOR DEFAULT:

The Competent Authority may, without prejudice to any remedy for breach of contract, by written notice of default sent to the Tenderer, terminate the agreement in whole or in part if:

- a) The Tenderer fails to perform any or all of the obligations within the time period specified in the agreement or any extension thereof granted by the Competent Authority.
- b) The quality of the delivery is not up to the satisfaction of the Competent Authority.
- c) The Tenderer fails to perform any other obligation under the agreement.
- d) The Tenderer fails to perform any other obligation, which the Competent Authority feels necessary for the best interest of the Purchaser.

The Competent Authority may at any time terminate the contract by giving written notice to the Tenderer without compensation to the Tenderer, if the Tenderer becomes bankrupt or otherwise insolvent, provided that such termination will not prejudice or affect any right of action or remedy, which has occurred thereafter to the Competent Authority. In case of termination of contract as mentioned above all Bank Guarantee furnished by Tenderer shall stand forfeited.

22. SUSPENSION:

The Competent Authority may by a written notice of suspension to the Tenderer, suspend all payments to the Tenderer if the Tenderer fails to perform any of its obligations (including the carrying out of the tasks) provided that such notice of suspension:

- A) Shall specify the nature of the failure and
- B) Shall direct the Tenderer to remedy such failure within a specified period from the date of receipt of such notice of suspension by the Tenderer.



23. PROPERTY AND RISK:

- a. The property and risk in the goods shall pass to the Competent Authority when they are delivered and accepted as of the FAT (Factory Acceptance Test) in accordance with the conditions of the agreement. Such passing of property and risk shall be without prejudice to any right of rejection.
- b. All goods must pass the acceptance test and Competent Authority shall be entitled to reject all or any goods, which do not conform completely in every respect to the specifications.
- c. If by the nature of the goods or property, any defect therein or any failure to conform as aforesaid does not or would not become apparent (despite the carrying out the examination and / or required test) until after use, Competent Authority may reject the same even after a reasonable period of use.
- d. Any goods rejected must at the request of Competent Authority be replaced or re- performed as the case may be, by the Tenderer at his expense. Alternatively, Competent Authority may elect to cancel the contract both in respect of the goods in question and of the whole of the undelivered balance (if any) of the goods covered under this contract. All rejected goods will be returned to Tenderer at his expenses.

24. ARBITRATION:

If any dispute of any kind whatsoever arise between M.P. Forest Department and the successful bidder in connection with or arising out of the contract, including without prejudice to the generality of the foregoing, any question regarding its existence, validity or termination, the parties shall seek to resolve any such dispute or difference by mutual consultation. If the parties fail to resolve such a dispute or difference by mutual consultation an appeal may be filed to the APCCF-IT, If still unresolved then, the dispute would be resolved as per MP Madhyastham Adhikaran Act, 1985. The place of arbitration shall be Bhopal and all legal disputes are subject to the jurisdiction of courts at Bhopal.

25. RIGHT OF INSPECTION:

- a) The Competent Authority shall have the right to inspect the work or get it inspected by its agent or any authorized officer at any stage.
- b) The supplier must have suitable facilities at his establishment / workshop / R & D center for carrying out various performance tests on the equipment's. A functional & reliability test may be carried out at the Tenderer's center or any other place decided by the competent authority.

26. PATENT, COPYRIGHTS, DESIGN, INTELLECTUAL PROPERTY RIGHTS AND INDEMNITY

LIABILITY:

- a. The Tenderer shall indemnify the Madhya Pradesh Forest Department for any third party liability arising out of patent or copyright or intellectual property or any other dispute. Tenderer shall bear the cost of any dispute arising as of alleged violation of any law and policy applicable in India, with respect to this supply.
- b. The Tenderer shall not purchase or use or offer the goods for the performance of work which would infringe any Indian or foreign patent, trademark, registered design or other intellectual



property rights, whether or not similar to any of the said goods

- x. That Tenderer shall indemnify the Competent Authority from all actions, costs, claims, demands, expenses & liabilities whatsoever resulting from any actual or alleged infringement as aforesaid and at the expenses of Tenderer shall be defended in the defense of any proceedings which may be brought in that connection.
8. No goods covered by the contract shall be manufactured, sold, disposed or done by Tenderer in violation of any right whatsoever of third party, and in particular, but without prejudice to the generality of the foregoing of any patent right, trademark or similar right, or of any charge, mortgage or lien.
- e. Tenderer should submit Certificate signed by O.E.M. regarding non-violation/no- infringement of any Indian or foreign patent, trademark, registered design or other intellectual property rights.

27. ASSIGNMENT AND SUBCONTRACTING:

- 1) Tenderer shall not assign or transfer this contract or part thereof to any other person without written consent of the Competent Authority.
- 2) Tenderer shall not, without the written consent of Competent Authority, subcontract this contract or part thereof.
- 3) For the purpose of the liabilities under this tender, the Tenderer will be considered assolely liable to all the components of the tender.

28. REGISTRATION WITH GST:

The bidder should have their firm registered with GST and shall furnish notarized copies of the same with their Pre-qualification bid along with their latest Tax clearance certificates from the concerned Purchaser.

29. OTHER CONDITIONS:

- The Competent Authority may cancel the tender and all proceedings relating there to, without assigning any reason. The decision of the Competent Authority shall be final as regards the acceptability of Tendered items and items supplied by the Tenderer and Competent Authority shall not be required to give any reason in writing otherwise at any time for rejection of the Tender or items.
- Any call deposit pending with the Purchaser in another connection cannot be adjusted for the present Tender.

30. SECURITY DEPOSIT:

- The successful Tenderer will be required to furnish a fresh Security Deposit equal to 03% of the Contract value in the shape of FDR / Bank guarantee issued by any Indian Nationalized/ commercial Bank at the time of execution of agreement
- After furnishing the security deposit by successful tenderer, the E.M.D. of fixed amount deposited with their bid of all other participating tenderers will be released.
- Security deposit will be returned to the vendor/supplier after expiry of warranty period.



31. AGREEMENT:

- ✓ The successful Tenderer will have to enter into an Agreement with the Madhya Pradesh Forest Department through APCCF (IT), for the material of the contract on Rs 1000/- non judicial stamped paper, within 15 days of the communication of the final order on bids, the cost of which has to be borne by the supplier. The Madhya Pradesh Forest Department shall provide Proforma for such an agreement. No variation is permitted in this agreement.
- ✓ Until such an agreement is signed, there is no liability for Madhya Pradesh Forest Department and Competent authority. APCCF (IT), (Competent Authority) may scrap the tender or any of its parts without assigning any reason at any time before the signing of the agreement. In case of scrapping of tender or its part the Competent Authority will not be liable for any loss or cost to tenderer. Till the signing of agreement, the tender shall bear its own cost for all the activities relating to this tender.
- ✓ This RFP will also be a part of agreement.
- ✓ Draft copy of the Agreement will be provided to the successful bidders.

32. confidentiality

The successful bidder shall ensure that all information obtained in relation to this tender, whether technical, commercial, or financial, is kept strictly confidential and is not disclosed to any person, firm, or organization without the prior written approval of the tendering authority.



33. Technical (ANNEXURE-1)

| SN | Description | YES/No | Page No |
|----|---|--------|---------|
| 1 | OEM or Authorized Partner of the proposed solution. In case of Authorized Partner, tender specific OEM MAF should be submitted at the time of bidding. | | |
| 2 | Successful execution of at least 2 similar projects in Government/PSU/large enterprises. Purchase Order/Work Order copies should be submitted for the same. | | |
| 3 | The bidder must have at least two certified engineers in the proposed EDR security software. OEM-issued certification proof must be submitted with the bid. | | |
| 4 | Valid GST, PAN, Incorporation or Gumashta certificates. | | |
| 5 | Average turnover of last 3 years 1Cr, CA Certified Turnover Certificate or Audited Balance sheet should be submitted at the time of bidding. | | |
| 6 | Technical compliance Annexure 2 in OEM Letter Head | | |
| 7 | Independent third-party test validation (AV-TEST, AV-Comparatives, SE Labs) proving high protection rates against ransomware and advanced threats. | | |



34. (ANNEXURE-2)

Technical Specifications- Endpoint Detection and Response

| S. No. | Functional requirements: | Compliance Yes/No |
|---------------|--|------------------------------------|
| 1 | Solution should support protection of the latest Operating Systems versions across all platforms (Windows, Linux, MacOS, iOS, Android). | |
| 2 | Solution should be able to detect Viruses (including polymorphic), Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, Phishing sites and links, Zero-Day Vulnerabilities and other malicious and unwanted software types of threat. | |
| 3 | Solution should support Anti-malware Scan Interface and provide next gen protection technologies such as protection against file- less threats, provision of multi-layered Machine Learning (ML) based protection and behaviour analysis during different stages of the kill-chain. | |
| 4 | Solution should be capable in Memory Scanning for Windows workstations and Kernel Memory Scanning for Linux workstations. | |
| 5 | Solution should have capability to switch to cloud mode for threat protection, decreasing RAM and hard disk drive usage for resource- limited machines. | |
| 6 | Solution should have dedicated components to monitor, detect and block activities on Windows, Linux and Windows servers, and endpoints, to protect against remote encryption attacks. | |
| 7 | Solution should have the ability to configure and manage firewall settings built into the Windows Server and Linux operating systems, through its management console. | |
| 8 | Solution should have the Application, Web and Device Controls, Anomaly Detection, HIPS and Firewall. | |
| 9 | Patch management, encryption components in a single agent installed on the endpoint. | |
| 10 | Solution should have Application and Device Controls for Windows workstations and Application Launch/Start Control for the Windows Server operating system. | |
| 11 | On detecting ransomware/cryptor-like activity solution should automatically block the attacking computer for a specified interval and list information about the attacking computer IP and timestamp, and the threat type. | |
| 12 | Solution should support the installation of endpoint protection on servers without the need to restart. | |
| 13 | Solution should be password-protected to prevent the AV process being halted/killed and for self-protection, regardless of the user authorization level on the system. | |
| 14 | Solution should be able to scan HTTPS, HTTP and FTP traffic against viruses and spyware, or any other malware. | |
| 15 | Solution should be firewall capable in order to block network activates of applications based on their categorization. Blocking/allowing specific packets, protocols, IP addresses ports and traffic direction. | |
| 16 | The automatic and manual addition of network subnets, and modification of network activity permissions. | |
| 17 | Solution should prevent the connection of reprogrammed USB devices emulating keyboards, and enable control of the use of onscreen keyboards for authorization. | |
| 18 | Solution should be able to block network attacks and report the source of the infection. | |
| 19 | Solution should have local storage on endpoints to keep copies of files that have been deleted or modified during disinfection. These files should be stored in a specific format that ensures they cannot pose any threat. | |
| 20 | Solution should support AM-PPL (Anti- Malware Protected Process Light) technology for protection against malicious actions | |
| 21 | Solution should include protection against attacks that exploit vulnerabilities in the ARP protocol in order to spoof the device MAC address. Solution should support Anti-Bridging functionality for Windows workstations to prevent unauthorized bridges to the internal network that bypass perimeter protection tools. Administrators should be able to ban the establishment of simultaneous wired and modem connections. | |



- 22 Solution should support dedicated component for scanning encrypted connections and ability to remotely wipe data on the endpoint.
- 23 Solution should have the ability to prioritize custom and on-demand scanning tasks for Linux workstations.
- 24 Solution should have the functionality to isolate infected computers and ability to automatically scan removable drives for malware when they are attached to any endpoint. Scan control should be based on drive size.
- 25 Solution should be able to differentiate between USB storage devices, printers, mobiles and other peripherals.
- 26 Solution should be able to log file operations (Write and Delete) on USB storage devices.
- 27 Solution should have ability to block/allow user access to web resources based on websites, content type, user and time of day. Solution should support user-based policies for Device, Web and Application Control.
- 28 Solution should have feature cloud integration, to provide the fastest possible updates on malware and potential threats.
- 29 Solution should support the blocking of prohibited (Deny- List) applications from being launched on the endpoint, and the blocking of all applications other than those included in Allow-Lists.
- 30 Solution should have the ability to allow applications based on their digital signature certificates, MD5, SHA256, META Data, File Path, and pre-defined security categories.
- 31 Solution should support Test Mode with report generation on the launch of blocked applications.
- 32 Solution should have the ability to restrict application activities within the system according to the trust level assigned to the application, and to limit the rights of applications to access certain resources, including system and user files “HIPS functionality”.
- 33 Solution should have endpoint mail threat protection with Attachment filter and the ability to rename attachments, scanning of mail messages when receiving, reading and sending.
- 34 Solution should enable the user of the computer to perform a check on a file’s reputation from the File Context menu.
- 35 Solution should have features scanning of all scripts.
- 36 Solution should have capability to provide protection against zero day malware based of the analysis of their behaviour and examination of changes in the system register, together with a strong remediation engine to automatically restore any system changes made by the malware.
- 37 Solution should provide protection against hacker attacks by using a firewall with an intrusion detection and prevention system (IDS/IPS) and network activity rules for more popular applications when working in computer networks of any type. Solution should support Ipv6 protocol.
- 38 Solution should have features Application Self-Protection technology eg. Protecting against unauthorized the remote management of an application service, protecting access to application parameters by setting a password and preventing the disabling of protection by malware, criminals or amateur users.
- 39 Solution shall have the antivirus checking and disinfection of files that have been packed using programs like PKLITE, LZEXE, DIET, EXEPACK, etc.
- 40 Solution should have the features such as anti-malware checking and disinfection of files in archives using the RAR, ARJ, ZIP, CAB, LHA, JAR, ICE formats, including password-protected files.
- 41 Solution shall have multiple ways to notify the administrator about important events which have taken place (mail notification, audible announcement, pop-up window, log entry).
- 42 Solution should allow to protect Exchange Online mailboxes, OneDrive users and SharePoint Online sites that are managed through Office 365 and detect critical information in files that are located in Office 365 cloud storages.
- 43 **Encryption:**
- 44 Solution should support encryption as Full disk encryption, File and folder encryption, Removable media encryption, BitLocker and MacOS Filevault2 Encryption Management



45 Solution should have functionality File Level Encryption (FLE) functionality that allows The encryption of files on local computer drives ,creation of encryption lists of files by extension or group of extensions and The encryption of all files stored on removable drives

46 Solution should have the capability to restore encrypted devices if an encrypted hard drive or removable drive is corrupted.

47 Solution should have the ability to centrally monitor encryption status and to generate reports regarding encrypted computers/devices. Having a central location for encryption key storage, and multiple recovery options.

48 Solution should support the automatic encryption of removable storage devices and able to prevent data being copied to unencrypted media.

49 Solution should have the functionality to manage/apply Microsoft Bit locker encryption.

50 Systems Management, vulnerability and patch management:

51 Solution should have features to manage computers remotely and

52 Solution have capability to monitor of the installation of unauthorized software Removal of unauthorized software

53 Solution should include patch management capabilities for Windows operating systems and for installed third-party applications. Solution management server should be configurable as an updates source for Microsoft Updates and third-party applications.

54 Solution should have the option to select which patches are to be downloaded/pushed to endpoints, based on their criticality.

55 Solution should be able to detect existing vulnerabilities in operating systems and other installed applications, and then to respond by automatically downloading/pushing the necessary patches to endpoints.

56 Solution should support patch aggregation to minimize number of updates needed.

57 Solution should support the automated distribution of patches and updates for 150+ applications.

58 Solution should have patch testing mode support functionality. Solution should support operating system deployment.

59 Solution should support Wake-on LAN and UEFI.

60 Solution should have built-in remote desktop sharing functionality. All file operations performed on the remote endpoint during the session should be logged on the Management Server.

61 Solution should be able to remotely push/deploy EXE, MSI, bat, cmd, MSP files, and allow the administrator to define the command line parameter for the remote installation.

62 Solution should be able to remotely uninstall applications, not limited to incompatible Anti- Virus programs.

63 Solution management server should be able to send logs to SIEMs and SYSLOG servers.

64 Solution should be able to track third party application licenses and raise notifications of any potential violations.

65 Centralized administration, monitoring and update software requirements :

66 Solution should enable the installation of anti- malware software from a single distribution package. Solution should support two-step verification for authentication.

67 Solution should have ability to read information from Active Directory to obtain data about computer accounts in the organization.

68 Solution should have a built-in web console for the management of the endpoints, which should not require any additional installation.

69 Solution should enable the management of a component controlling user activity on the internet.

70 Solution should be capable to automatically deploy protection to virtual infrastructures based on VmwareESXi, Microsoft Hyper-V, Citrix XenServer virtualization platform or hypervisor.

71 Solution should have the ability to specify any computer in the organization as a center for relaying updates and installation packages, in order to reduce the network load from administration server system.

72 Solution should be able to export of reports to PDF and XML files. Solution Should have a built-in clustering feature & support Windows Failover Cluster.



- 73 Solution should have Role Based Access Control (RBAC) and restrictions to be replicated throughout the management servers in the hierarchy. It should have pre-defined security roles for the Auditor, Supervisor and Security Officer.
- 74 Solution's management server should maintain a revision history of the policies, tasks, packages, management groups created, so that modifications to a particular policy/task can be reviewed.
- 75 Solution should have support notification through Email, Syslog, SIEM.
- 76 Solution should have the ability to create/define settings based on a computer's location in the network, rather than the group to which it belongs in the management server.
- 77 Solution should support OPEN API, and include guidelines for integration with 3rd party external systems.
- 78 Solution should have built-in tool to perform remote diagnostics and collect troubleshooting logs without requiring physical access to the computer.
- 79 Solution should have the option for the customer to either deploy an on-premises management console, or use the vendor- provided cloud-based management console.
- 80 Solution should support industry standard SIEM solutions eg. HP (Microfocus), ArcSight, IBM Qradar, Splunk, Syslog.
- 81 **EDR Capabilities :**
- 82 Solution should support integration with APT solution.
- 83 The suggested solution should support integration with Managed Detection and Response service.
- 84 Solution should support integration with threat intelligence portal, which contains and displays information about the reputation of files and URLs.
- 85 The suggested solution should support central management and analytics through on-prem Web console. (Incident related data, System status and health check data, Settings, etc.)
- 86 EDR agent should have integration with Endpoint Protection application (Single agent). EDR and Endpoint Protection solutions should have unified console for administrators and analysts.
- 87 Solution should support automated detection of malicious activity using Endpoint Protection solution.
- 88 Solution should support auto generation of threat indicators (IoC) after detection occurs with ability to apply response action.
- 89 Solution should have the capability to force run IoC scan across all endpoints with installed EDR agents.
- 90 Solution should support import of third-party IoC in OpenIoC format for its use in network scanning.
- 91 Solution should generate detailed incident card related to the detected threat on an endpoint.
- 92 Threat development chain (kill chain) graph should provide visual information about the objects (about key processes on the device, network connections, libraries, registry, etc) involved in the incident, for example.
- 93 Solution should provide 'Single-click" response from management console and response guidance (guided response).
- 94 Solution Should support the Prevent object execution, response, Host isolation actions, Delete object from host or group of hosts, Terminate a process on the device, Quarantine an object, Run system scan, Remote program / process / command execution and start IOC scan for a group of hosts that an administrator can perform when threats are detected.
- 95 Solution Should be also includes mobile security licenses as well
- 96 It should be covered automated security training for IT security team.



35. (ANNEXURE-2)

Tender Acceptance Undertaking
(To be submitted on letterhead of tenderer)

To,

**Additional Principal Chief Conservator Of Forests,
Office of Principal Chief Conservator Of Forest(HoFF)
Wing-Information Technology
Second floor, "C" Block,
Van Bhawan, Tulsi Nagar,
Bhopal-462004.**

Tender Ref No.:..... Date:

Antivirus Endpoint Detection and Response(EDR) for network security.

Dear Sir/Madam,

1. I/We have downloaded/obtained the tender documents for the above-mentioned tender work.
2. I/We hereby certified that I/We have read the entire terms and conditions of the tender documents including all Annexure/schedule etc. which form the part of the contract/agreement and I/we shall abide here by the terms, conditions and clauses contained therein.
3. I/We hereby unconditionally accept the tender conditions of above-mentioned tender document/corrigendum in its totality/entirety.
4. I/We do hereby declare that our firm has not been black listed/debarred by any government department/ public sector undertaking/government organization.
5. I/ we certified that all information furnish by our firm is true and correct and, in the event, that the information is found to be incorrect/untrue or found violated then your center shall without giving any notice or reason therefor or summarily reject the bid or terminate the contract, without prejudice or remedy including the forfeiture of the full said EMD absolutely.

Your Faithfully

Signature of tenderer with stamp

Name
Address

Date:

*** For any query contact**

Office Of Principal Chief Conservator Of Forests(HoFF)
Wing Information Technology
2nd floor, "C" Block, Van Bhawan, Tulsi Nagar, Bhopal-462004.
email:apccfit@mp.gov.in , Phone 0755-2674302,2524302