ASSAM POWER GENERATION CORPORATION LIMITED
Registered Office: Bijulee Bhawan, 3rd floor, Paltanbazar, Guwahati-781 001, Assam.
Email: md.zakir@apgcl.org, Tele-Fax: 0361-2739522.

A. Saikia, (CISO), APGCL

Notice No: APGCL/CISO/2025-26/End Point Security (Antivirus)/01 **Date:** 06 /12/2025

NOTICE INVITING TENDER (NIT)

The CISO, APGCL, Bijulee Bhawan, Paltanbazar, Guwahati-1 invites sealed tenders from eligible firms to carry out the work of *"Supply and Installation of End Point Security (Antivirus) solution with Cloud Based Centralized Management Console at Assam Power Generation Corporation Limited".*

1. ELIGIBILITY OF THE BIDDER:

a) The participating bidder should be OEM of the offered End Point Security (Antivirus) solution or an authorized vendor/reseller/distributor of the OEM. **If the participating bidder is an authorized vendor of the OEM than the bidder should submit an authorization letter from the OEM.**

b) The OEM of the offered product should have **ISO 20000-1:2018, ISO 27001:2013, ISO 9001:2015** certified or its latest version of certification. Necessary documents to be submitted in this regard.

c) The participating bidder should not have been black listed by any State Govt., State/Central PSU or any other organization. In this regard bidder should submit a notarized document as per the format attached in **Annexure-I** in **Rs. 50 non-judicial Stamp Paper.**

d) The OEM of the offered product should have PAN INDIA presence. In this regard the participating bidder shall submit the necessary details.

e) The participating bidder should have average annual turnover of at least Rs. 2.65 Lakh only (Rupees two lakh sixty-five thousand only) during the FY 2022-23, 2023-24 & 2024-25. In this regard, the participating bidder shall submit Chartered Accountant (CA) certified average annual turnover document for FY 2022-23, 2023-24 & 2024-25. Such CA certified document shall include Balance Sheet, Profit & Loss Statement and Cash Flow Statement of the above-mentioned relevant years.

2. EXPERIENCE OF THE BIDDER:

a. The **Offered Product of the Bidder in this Tender** should have been supplied to at least **03 (three) nos.** of Govt. Department/PSU/Private Organization Clients in last 05 (five), with at least 100 user licenses with a support for a period of at least 01 (one) year.

Note: The above mentioned past 05 years period shall be calculated from the start date of bid submission against this tender. Necessary documentary evidence in this regard – i.e., Work Order copies wherein the technical specifications of the supplied product is mentioned and Work Completion Reports from Clients are to be submitted with the tender or an Undertaking from the OEM of the Offered Product mentioning Client Names with contact details to whom the offered product with at least 100 user licenses and with a support for a period of at least 01 (one) year has been supplied in last 5 years can also be submitted.

b. The **participating bidder** should have at least 01 (one) experience in supply and installation of IT security systems in any Govt. Department/PSU/Private Organizations during the last 05 (five) years. In this regard, the bidder shall submit a copy of previous Work Order and Work Completion Report from his client in support of his experience.

Note: The above mentioned past 05 years period shall be calculated from the start date of bid submission against this tender.

3. **TECHNICAL SPECIFICATION: The offered products of bidder must fully comply with the technical specifications mentioned in Table A & B of this document and bidder shall submit a signed & sealed confirmation in this regard in his submitted tender. In case the offered product doesn't match the below given specifications, the bid of such bidder will be rejected.**

TABLE-A

Sl. No.	Description: End Point Security Software to protect Desktops/Laptop & Servers with following functionality for 350 (Approx) users with Cloud Based Centralized Management Console
1	End Point Security Solution Should have a Cloud based Centralized Management Console for both Servers & desktop/laptop
2	The End Point Security solution should provide protection for desktops & servers of all the attacks originating from places inside/outside of the network due to viruses and/or other malicious programming code.
3	The End Point Security solution should Support Multi-Platform operating system (Windows, Mac & Linux) .and the same should be managed from a single cloud based Centralized Management console.
4	Solution should have an application-based console.
5	End Point Security Solution should have single, Configurable Installation with centralized configuration & policy management.
6	Automatic update of End Point Security from Original Software Developer (OSD)/Original Equipment Manufacturer (OEM) & the client should get update from the local Server If updating from the Primary Server fails for any reason (such as the user being off the network) an attempt should be made to contact the Secondary Server (i.e., OSD/OEM).
7	End Point Security should have centralized scanning of all network Systems
8	Administrator should have flexibility to schedule Scan and update at the endpoints from central Server.
9	End Point Security should be able to capture Viruses, Trojans, Worms, Spyware and Malware, adware and Potentially Unwanted Application (PUA) from single agent.
10	End Point Security Should have Host Intrusion Prevention System (HIPS)technology which works in 4 Layers to provide zero-day protection without the need for updates (Unknown Virus Detection & Repair).
11	End Point Security should have run time detection technology i.e., behavioural & Heuristic scanning to protect from unknown viruses and buffer overflow protection integrated with AV scan engine for protection from threats/exploits that uses buffer overflow
12	End Point Security Software must have the capability to clean, Quarantine or delete Viruses and should be able to detect new classes of viruses by normal virus definition update mechanisms
13	End Point Security OSD/OEM should provide definitions with incremental updates. Should support daily updates for definition files. Size of daily update should be extremely small in size and solution must provide update/relay agent capability.
14	Administrator should be able to add files, folders or extensions to an exclude list so that they are not scanned on access.
15	Administrator should be able to lock down all End Point Security configurations at the desktop & User should be prevented from being able to uninstall the anti-virus software.
16	Administrator must be able to distribute new and update End Point Security software, virus definitions and Policies automatically to clients and servers from a central console
17	End Point Security should provide centralized event logging to locate and cure virus
18	Alerts on virus activity should be passed on to administrator
19	End Point Security Should have Personnel Firewall (Client Firewall) with location awareness feature, and it should block unsolicited inbound traffic, control outbound traffic, and apply policy rules based on traffic, ports, IP Address and Domain Name.

20	End Point Security should have a Live web protection module Integrated into existing endpoint agent with no endpoint configuration required to Blocks URLs that are hosting malware and Should Support all major browsers - IE, Firefox, Safari, Opera, Chrome etc.
21	Solution Updates should be minimal in kb/mb to Reduce Minimum impact on Bandwidth and solution must provide update/relay agent capability.
22	Solution must support Device Blocking and Exceptions with Vendor and Model (Device ID), with the option of Block/Read/Allow.
23	OEM should have End Point Security scanner for USB access for all supported Operating Systems of Windows & Mac.
24	OSD/OEM Should have 24x7 toll free Global Technical Support.

OTHER SPECIAL CONDITIONS: -

TABLE-B

Sl. No.	Technical Specification (Endpoint Security – Cloud Based)
1	Must offer comprehensive endpoint security by providing virus protection, spyware, rootkits, bots, grayware, adware, malware and other computer borne threats or mixed threat attacks or any emerging cyber-attacks or zero-day attack protection.
2	Solution must clean computers of file-based and network viruses plus virus and worm remnants (Trojans, registry entries, viral files) through a fully-automated process.
3	Must be able to reduce the risk of virus/malware entering the network by blocking files with real-time compressed executable files.
4	Must include capabilities for detecting and removing rootkits
5	Must provide Real-time spyware/grayware scanning for file system to prevent or stop spyware execution
6	Must have capabilities to restorespyware/grayware if the spyware/grayware is deemed safe
7	Must have Assessment mode to allow first to evaluate whether spyware/grayware/ malware is legitimate and then take action based on the evaluation
8	Solution must provide these capabilities in a single agent: antimalware, application control, virtual patching, host firewall, URL reputation-based blocking, machine learning, behaviour monitoring, USB blocking, ransomware protection.
9	To address the threats and nuisances posed by Trojans, the solution should be able to do the following but not limited to: a) Terminating all known virus processes and threads in memory b) Repairing the registry c) Deleting any drop files created by viruses d) Removing any Microsoft Windows services created by viruses e) Restoring all files damaged by viruses Includes Clean-up for Spyware, Adware etc.
10	Must be capable of cleaning viruses/malware even without the availability of virus clean- up components. Using a detected file as basis, it should be able to determine if the detected file has a corresponding process/service in memory and a registry entry, and then remove them altogether.
11	Must provide suitable Outbreak Prevention Solution either through limit/deny access to specific shared folders, block ports, and deny write access to specified files and folders on selected customers or equivalent features in case there is an outbreak.
12	Behaviour Monitoring: Must have behaviour monitoring to restrict system behaviour, keeping security related processes always up and running
13	Users with the scheduled scan privileges can postpone, if admin wants can skip, and stop Scheduled Scan.
14	CPU/memory (physical or virtual) usage performance control during scanning: a) Checks the CPU usage level configured on the Web console and the actual CPU consumption on the computer b) Adjusts the scanning speed.

	c) The CPU usage level is High, Medium or Low Actual CPU consumption exceeds a certain threshold
15	Should have a manual outbreak prevention feature that allows administrators to configure USB ports control (Open/Close for use) and deny writes to files and folders manually
16	Should have the capability to assign a customer the privilege to act as an update/master relay agent for rest of the agents in the network
17	Shall be able to perform different scan Actions based on the virus type (Trojan/ Worm, Joke, Hoax, Virus, other)
18	Shall be able to scan only those file types which are potential virus carriers (based on true file type)
19	Should be able to detect files packed using real-time compression algorithms as executable files.
20	Shall be able to scan Object Linking and Embedding (OLE) File
21	Must provide Web threat protection by the following ways: a) Must be able to protect the endpoints from Web threats by blocking access to and from malicious sites based on the URL's reputation ratings b) Must extend Web threat protection to the endpoints even when they disconnect from the network, i.e. regardless of the location c) Must have the capabilities to define Approved URLs to bypass Web Reputation policies d) Must provide real-time protection by referencing online database with millions of rated Web domains e) Configure Web reputation policies and assign them to individual, several, or all end users machine.
22	Must protect endpoints on the network from high performance network virus, & do scanning and elimination
23	Must provide the flexibility to create firewall rules to filter connections by IP address, port number, or protocol, and then apply the rules to different groups of users and provide full disk encryption.
24	Must have smart feedback to enable feedback from the customer agents to the threat research Centres of the vendor.
25	Uses any alternate method other than the conventional pattern- based scanning with the following features: a) Provides fast, real-time security status lookup capabilities in the cloud b) Reduces the overall time it takes to deliver protection against emerging threats c) Reduces network bandwidth consumed during pattern updates. The bulk of pattern definition updates only need to be delivered to the cloud or some kind of repository and not to many endpoints Lowers kernel memory consumption on endpoints. Consumption increases minimally over time.
26	Should be able to deploy Customer software using the following mechanisms: a) Customer installation Package (Executable & Microsoft Installer (MSI) Package Format), should support silent installer, unmanaged customers, specific installer for servers b) Web install page c) Login Script Setup d) Remote installation e) Standalone Installer. f) Email Install Link
27	Must provide a secure Web-based management console to give administrators transparent access on the network
28	The management server should be able to download updates from different source if required.
29	Must reduce network traffic generated when downloading the latest pattern by downloading only incremental patterns.
30	Must have the flexibility to roll back the Virus Pattern and Virus Scan Engine if required via the web console
31	Should have scope for role-based administration with active directory integration
32	Should have scope for integration with the latest Active directory version
33	Shall support grouping of customers into domains for easier administration.

34	Establish separate configuration for internally versus externally located machines (Policy action based on location awareness)
35	Must be capable of uninstalling and replacing existing customer antivirus software and to ensure unavailability of any residual part of the software.
36	Security Compliance should leverage Microsoft Active Directory services to determine the security status of the computers in the network
37	Should have a feature similar to Firewall Outbreak Monitor which sends a customized alert message to specified recipients when log counts from customer IPS, customer firewall, and/or network virus logs exceed certain thresholds, signalling a possible attack.
38	Must be able to send a customized notification message to specified recipients when firewall violations exceed certain thresholds, which may signal an attack
39	Virus definition files should be lighter so that same can be transmitted to remote locations.
40	System should be configured with the option that endpoints can get updated directly from internet or from local security server. This option can be used with flexibility to allow end point to get update from internet or block to stop update from internet.
41	In case of bot infection, bot removal tools also to be facilitated to clean the infected machine and solution should have the option of the endpoint vulnerability shielding in the network.
42	The solution should have latest machine learning technology in built from day one and solution should have ransomware protection in built.
43	The Solution must support both IPV4 & IPV6
44	The validity of the licenses of the solution should be 1 year from date of commissioning.
45	The Solution should be MeitY Complaint. The cloud-based centralized management console for the Endpoint Security solution must be hosted within India and all related data must reside in India.
46	The Solution should have its own indigenous developed antivirus scan engine.

4. SCOPE OF WORK OF THE BIDDER:

The scope of work of the bidder shall be Supply and Installation of End Point Security (Antivirus) solution with Cloud Based Centralized Management Console at Assam Power Generation Corporation Limited.

a) **SCOPE OF SUPPLY:** Bidder shall supply the below mentioned items:

Sl. No.	Items Description	Quantity
1.	End Point Security (Antivirus) solution with Cloud Based Centralized Management Console.	Around 350 nos.

b) **SCOPE OF SERVICE:**

The scope of Service of the bidder shall be Installation of the supplied End Point Security (Antivirus) solution with Cloud Based Centralized Management Console at various locations of Assam Power Generation Corporation Limited (i.e., at Headquarter and various power plants of APGCL).

NOTE:

a) The number of the users for the End Point Security with Centralized Management Console (Cloud based) is **approx. 350 nos. However, the number of users may increase/decrease depending on the requirement and the successful bidder must provide the same at the same his offered rate and as per terms & conditions of this tender.**

b) APGCL reserves the right to increase or decrease quantity and/or amount of work. Decision on Quantity of material by APGCL will be final in this regard.

5. OTHER TERMS AND CONDITIONS:

5.1 FIRM PRICE:

The price(s) quoted by the bidder shall be Firm without any variation in any way till completion of the work in full and should be inclusive of all other charges viz. freight, transit insurance, P&F, travelling charges, etc.

GST shall be clearly quoted by bidder in his offered price.

Note: Guest House accommodation, subjected to availability, with maximum two double-bedded rooms can be arranged on Chargeable basis for contractor's personnel during work execution at APGCL Power Plant Sites located outside Guwahati.

Note: The bidder shall quote the price as per the format attached in **Annexure-II.**

5.2 VALIDITY OF BID:

The prices quoted by the bidders shall be valid for a period of **180 (One Hundred Eighty) days** from the start date of tender submission.

5.3 EVALUATION AND COMPARISON OF BID:

The Bid Evaluation Committee of the Procuring Entity (APGCL) shall evaluate the Bidder's submitted Tender based on the criteria/Terms & Conditions of this Tender.

The L1 bidder shall be selected based on the lowest total price offered (i.e., inclusive of GST, any other tax and duties, etc.) in BoQ and subject to fulfillment of Bid Criteria given in this document.

5.4 CLARIFICATION AND ADDITIONAL INFORMATION:

During the submitted bid's evaluation, APGCL may request the bidder for any clarification on the submitted bid and/or documents related to the tender. The bidder shall submit the sought clarifications and/or document(s) within stipulated time as determined by the undersigned. However, seeking clarification and document(s) during bid evaluation shall be on sole discretion of APGCL. All such clarifications shall be requested by APGCL and submitted by Bidder through official email of the respective entity. Hence, bidder shall provide his official email Id in his submitted bid for communication purpose.

5.5 SETTLEMENT OF DISPUTES:

a. AMICABLE SETTLEMENT:

If any dispute or difference (s) of any kind whatsoever arise between the parties in connection with or arising out of the work/contract, including without prejudice to the generality of the foregoing, any question regarding its existence, validity or termination, or the execution of the Contract whether during the progress of the Contract or after its completion and whether before or after the termination, abandonment or breach of the Contract, the parties shall seek to resolve any such disputes or differences by mutual consultation between the authorized representatives of both the parties for amicable settlement of the dispute within a period of ninety (90) days after receipt by one party of the other party's request for such amicable settlement.

b. ARBITRATION:

Any dispute, controversy or claim arising out of or relating to this work/contract or the breach, termination or invalidity thereof, that cannot be settled amicably between both the parties shall be settled by Arbitration.

In any arbitration proceeding hereunder-

i. Arbitration shall be in accordance with the Arbitration & Conciliation Act, 1996 or any statutory amendment thereof.

ii. Arbitration shall be by a sole arbitrator, if agreed upon by the Parties. Failing agreement on the identity of such sole arbitrator, each Party shall appoint one arbitrator, and these two appointed arbitrators shall jointly appoint a third arbitrator, who shall chair the arbitration panel and act as the Presiding Arbitrator.

iii. In an arbitration proceeding consisting of three arbitrators, if a party fails to appoint an arbitrator within 30 days from the receipt of a request to do so from the other party; or the two appointed arbitrators fail to agree on the third arbitrator within thirty days from the date of their appointment, the appointment shall be made upon request of a party by the High Court or by the President, Institution of Engineers (India), Assam State Centre.

iv. In an arbitration with sole arbitrator, if the parties fail to agree on the arbitrator within 30 days from receipt of a request by one party from the other party to so agree, the appointment shall be made, upon request of a party, by the High Court or by the President, Institution of Engineers (India), Assam State Centre.

v. Proceedings shall, unless otherwise agreed by the Parties, be held in Guwahati.

vi. English language shall be the official language for all purposes.

vii. Decision of the sole arbitrator or of a majority of the arbitrators (or of the third arbitrator if there is no such majority) and the Arbitral Award shall be final and binding on the parties and the persons claiming under them respectively and shall be enforceable in any court of competent jurisdiction, and the Parties hereby waive any objections to or claims of immunity in respect of such enforcement.

viii. The arbitrators and the parties to the arbitration shall maintain confidentiality of all arbitral proceedings except award where its disclosure is necessary for the purpose of implementation, enforcement and setting aside of the award.

ix. The cost of arbitration shall be equally shared among both the parties.

5.6 LEGAL JURISDICTION:

Any disputes or differences arising under, out of, or in connection with this work/contract, shall be subject to the exclusive jurisdiction of courts at Guwahati only.

5.7 TERMS OF PAYMENT:

90% amount of the total work order value shall be made after successful supply and installation of the supplied antivirus software in all the servers & desktops/laptops installed in the APGCL (i.e., at APGCL Headquarter, Plant Sites, etc.)

Remaining 10% shall be made after 365 days of successful completion of installation of the supplied antivirus software at APGCL. This 10% amount of the total work order value shall be retained by APGCL as a performance security deposit.

Paying Authority:

The General Manager (F&A) i/c, APGCL,
3rd Floor, Bijulee Bhawan, Paltan Bazar,
Guwahati-781001.

Note:

- All bills are to be processed through the CISO, APGCL.

5.8 CONSIGNEE:

Sl. No.	Consignee Address	Contact Details
1	Prarthana Kalita, AGM (IT), Assam Power Generation Corporation Limited (APGCL) (Headquarter), 3rd Floor, Bijulee Bhawan, Paltan Bazar, Ghy-01.	E-mail: prarthana.kalita@apgcl.org Ph. No.: 8638170156.
2	Jadupran Borgohain, General Manager, Namrup Thermal Power Station, APGCL, Namrup, Dibrugarh, Assam, 786622.	E-mail: jadupran.borgohain@apgcl.org Ph. No.: 9435597454
3	Janardan Das, General Manager, Lakwa Thermal Power Station, APGCL, Maibella, Dist.- Charaideo, Assam, 785689.	E-mail: janardan.das@apgcl.org Ph. No.: 9435529107

4	Longsing Bey, General Manager, Karbi Langpi Hydro Electric Project & MSHEP Stage I & II, Lengery. District: West Karbi Anglong, PO: Amtreng, Assam – 782450.	E-mail: longsing.bey@apgcl.org Ph. No.: 9435361372
5	Jonardan Rongpi, Project Manager, Lower Kopili Hydro Electric Project Longku, Dima Hasao, Assam	E-mail: jonardan.rongpi@apgcl.org Ph. No.: 8638014206
6	Amarendra Singha, General Manager, Design (Civil), APGCL Narengi, Guwahati-781026	E-mail: amarendra.singha@apgcl.org Ph. No.:8062595863.
7	Aswini Choudhury, Deputy General Manager Investigation Circle, APGCL Narengi, Guwahati-781026	E-mail: aswini.choudhury@apgcl.org. Ph. No.:9401159235
8	Manokh Das, Assistant General Manager, Borpani Killing Valley (BKV) Investigation Division, Jagiroad APGCL	E-mail: manokh.das@apgcl.org Ph. No.:9531113323

5.9 WORK COMPLETION PERIOD:

The Work Completion Period for the **entire work of supply and installation** of End Point Security (Antivirus) solution with Cloud Based Centralized Management Console at Assam Power Generation Corporation Limited shall be **20 (twenty) days** from the date of issue of the Work Order by APGCL.

Liquidated damage due to delay in completion of the supply & installation work shall be levied as per the Liquidated Damage Clause of this tender.

5.10 MANDATORY DOCUMENTS:

The bidder must submit the hard copies of the following mentioned documents along with the technical bid, failing which the submitted bid of the bidder may be treated non-responsive.

a) Copy of PAN Card
b) Copy of GST Registration Certificate of the bidder's Firm
c) The participating bidder shall submit confirmation that their offered product conforms to the technical specifications mentioned under Clause 3 of this document.
d) Documents related to bidder's eligibility and past experience.
e) Documents related to bidder's Firm: Certificate of registration of the Firm (in case of Solo Proprietor)/Partnership Deed (in case of LLP)/Certificate of Incorporation (in case of Company), Joint Venture Agreement, whichever is applicable. Note: In case of Joint Venture (JV), the bidder must be the Lead Partner in the JV.
f) CA Certified Documents related to the bidder's average annual turnover during 03 (three) Financial Year (FY 2022-23, 2023-24 & 2024-25).
g) Authorization Letter (s)/Reseller/Distributorship certificate in case the bidder is not the OEM of the offered products.
h) ISO 20000-1:2018, ISO 27001:2013, ISO 9001:2015 certified or to its latest version of certification of the OEM.
i) Notarized Undertaking of the bidder of not being blacklisted.
j) Power of Attorney Letter to sign the bid document.
k) Any other document required as per this tender.

5.11 LIQUIDATED DAMAGE (LD):

The date of delivery/completion of work shall be deemed to be the essence of the contract and shall be completed not later than the date specified in the purchase order/contract. In case of failure to deliver the material/equipment/complete the work in full or to complete the delivery/complete the work within the stipulated delivery period or delay in the erection work beyond completion schedule, the Purchaser/Employer (APGCL) shall be entitled to: -

- Recover an amount at the rate of 1% (one percent) of the Contract Price/Work Order value per week or part thereof of delay, subjected to maximum of 10% (ten percent) of the Contract Price/Work Order value of Material/Work/Service delayed as Liquidated Damage. However, the payment of liquidated damage shall not in any way relieve the Contractor from any of its obligation to complete the work or from any other obligation and liabilities of the Contractor under the Contract/as per work order.
- Purchase the undelivered material/equipment from elsewhere or to complete the balance work, giving notice to the Contractor and to recover any extra expenditure incurred thereby for having to purchase these materials or complete the work at a higher price, at risk and responsibility of the Contractor.
- Cancel the Contract/Work Order wholly or in part and to purchase materials/equipment and execute the work at the full risk and cost of the Contractor and forfeit the security deposit.

The Start Date of Tender Submission is from 08/12/2025 from 10.00 hours.
The sealed tenders shall be dropped & submitted **in the Tender Box** located in the Office of the **Chief General Manager (Generation), APGCL, 3rd Floor, Bijulee Bhawan, Paltanbazar, Guwahati-781001** **on or before** **15.12.2025 up to 15:00 Hrs**.

The sealed tenders received shall be opened on the same date i.e., **15.12.2025 at 16:00 Hrs.** at Office of **CISO, APGCL**. The participating bidders or their authorized representatives may be present at the time of opening of the sealed tenders.

The participating bidder shall superscribe the envelope with the following information:

1. **Tender Title/Name of Work:**
2. **Notice Number:**
3. **Due Date & Time of submission:**
4. **Name and address of the bidder:**

Note:

All the documents submitted by the bidder must bear clear sign & seal of the Bidder on all the pages without which the submitted documents may not be considered for evaluation. Also, Power of Attorney Letter to sign the bid document issued from competent authority of Bidder must be submitted along with the bid. The person named in the Power of Attorney document must sign on all the pages of the submitted bid of bidder.

Saikia
CISO, APGCL,
Bijulee Bhawan, Guwahati-1

Memo No: APGCL/CISO/2025-26/End Point Security (Antivirus)/01 Date: 06 /12/2025

Copy to:

1) OSD to The Chairman, APGCL, Bijulee Bhawan, Paltanbazar, Guwahati-1, for favour of kind information of the Chairman.

2) OSD to The Managing Director, APGCL, Bijulee Bhawan, Paltanbazar, Guwahati-1, for favour of kind information of the Managing Director.
3) The Chief General Manager (Gen/F&A), APGCL, Bijulee Bhawan, Paltanbazar, Guwahati-1, for kind information.
4) The Deputy General Manager (F&A/Proc), APGCL, Bijulee Bhawan, Paltanbazar, Guwahati-1, for information & necessary action.
5) The Assistant General Manager (IT), APGCL, Bijulee Bhawan, Paltan Bazar, Guwahati-1, for information & necessary action
6) Notice Board.
7) Relevant File.

CISO, APGCL,
Bijulee Bhawan, Guwahati-1

Annexure-I

Undertaking by the Bidder

Affidavit

(To be submitted on non-judicial stamp paper of minimum Rs 50/- duly certified by Notary)

We, M/s. .... (the Bidder), (the names and addresses of the registered office) hereby certify and confirm that:

a) We or any of our promoter(s) /director(s)/partner(s) are not blacklisted or otherwise disqualified pursuant to any debarment proceedings by any Central or State Government, Local Government or Public Sector Undertaking in India from participating in any bidding process, either individually or as member of a consortium as on the_______ (Date of Signing of Bidder).
b) We are not insolvent, in receivership, bankrupt, being wound up, having our affairs administered by a court or a judicial officer, having our business activities suspended or subject of legal proceedings for any of the foregoing reason;
c) We or any of our promoter(s), director(s), partner(s) and officers are not convicted of any criminal offence related to their professional conduct or the making of false statements or misrepresentations as to their qualifications to enter into a procurement contract within a period of *three years* preceding the commencement of the procurement process.
d) There is no conflict of interest in submitting this Bid.
e) We shall abide by the clauses/ conditions of Bidding Documents issued by the Procuring Entity and any amendment made thereafter.

We further confirm that, we are aware of the fact that, our Bid submitted in response of the Tender Ref. No. [*insert tender number &date*] for [*insert the name of the Goods/subject matter of the Tender*], would be liable for rejection in case any material misrepresentation is made or discovered at any stage of Bid evaluation or thereafter during the agreement period.

Signature of the Bidder/Authorized Representatives

Name of the Bidder/Authorized Representatives

Annexure-II

PRICE BID FORMAT (BoQ)

Sl. No.	Item Description	Qty	UOM	Rate (in Rs.)	GST (%)	Unit GST (in Rs.)	Unit Total Amount (in Rs.)
1	Supply of End Point Security (Antivirus) solution with Cloud Based Centralized Management Console.	1	No.				
2	Installation Charges per License across Assam	1	No.				
UNIT TOTAL							
(In Words)							

(i.e., Unit Rates to be quoted by bidder as per the above BoQ Format).

Note:

a) No price escalation shall be considered on the quoted rate. Any other expenses required for completion of the work as per scope of work of bidder shall be borne by bidder without any cost implication on APGCL.

b) The number of the users for the End Point Security with Centralized Management Console (Cloud based) is approx. 350 nos. However, the number of users may increase/decrease depending on the requirement and the successful bidder must provide the same at the same offered unit rate of bidder & terms and conditions of this tender.

c) APGCL reserves the right to increase or decrease quantity and/or amount of work. Decision on Quantity of material by APGCL will be final in this regard.