THE INSTITUTE OF Company Secretaries of India
भारतीय कम्पनी सचिव संस्थान
IN PURSUIT OF PROFESSIONAL EXCELLENCE
Statutory body under an Act of Parliament

THE INSTITUTE OF COMPANY SECRETARIES OF INDIA
'ICSI HOUSE', C-36, SECTOR-62, NOIDA -201309

Tender No: PC/IT/Anti-Virus/2019 **13th May, 2019**

Sub: Procurement of Endpoint Protection Anti-Virus Software (Academic Version) Latest Version and Annual Onsite Comprehensive Maintenance Support.

Tender Fee	Rs. 236/-(Rs. 200/- + 18%GST) (Rupees Two Hundred Thirty Six only)
Earnest Money Deposit (EMD)	Rs. 24,000/- (Rupees Twenty Four Thousand only)
Tender Publish Date	13th May, 2019
Last Date and Time for Submission of Bids	27th May, 2019 by 2:00 PM
Address for submission of Bids	The Institute of Company Secretaries of India ICSI House, C-36, (Ground Floor: tender box) Sector-62, Noida – 201309
Venue, Date and time of opening of Technical Bids.	Address as above. Date: 27th May, 2019 at 3:00 PM
Bid Validity	90 days after the date of opening of Technical Bids
Contact details	**Dr. Nikhat Khan, Director, IT** (Tel. No. 0120-4522019, may be contacted).

Statement of Confidentiality

The information contained in this Tender Document or subsequently provided to Bidder(s) or applicants whether verbally or in documentary form by or on behalf of Institute of Company Secretaries of India (hereinafter "Institute" / "ICSI") or by any of its employees or advisors, shall be 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. The purpose of this RFP document is to provide the Bidder(s) with information to assist the formulation of their proposals. This Tender Document does not purport to contain all the information each bidder may require. This Tender document may not be appropriate for all persons, and it is not possible for the ICSI, its employees or advisors to consider the investment objectives, financial situation and particular needs of each bidder who reads or uses this Tender document. Each bidder should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information in this Tender document and where necessary obtain independent advice from appropriate sources. ICSI, its employees and advisors make no representation or warranty and shall incur no liability under any law, statue, rules or regulations as to the accuracy, reliability or completeness of the Tender document. ICSI may in their absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this Tender document.

THE INSTITUTE OF Company Secretaries of India
भारतीय कम्पनी सचिव संस्थान
IN PURSUIT OF PROFESSIONAL EXCELLENCE
Statutory body under an Act of Parliament

THE INSTITUTE OF COMPANY SECRETARIES OF INDIA
'ICSI HOUSE', C-36, SECTOR-62, NOIDA -201309

Tender No: PC/IT/Anti-Virus/2019 **13th May, 2019**

Sub: Procurement of Endpoint Protection Anti-Virus Software (Academic Version) Latest Version and Annual Onsite Comprehensive Maintenance Support.

About ICSI:

The Institute of Company Secretaries of India (ICSI) is a statutory body constituted under an Act of Parliament i.e. the Company Secretaries Act, 1980 (herein after referred as ICSI / Institute). ICSI is functioning under the overall administrative jurisdiction of Ministry of Corporate Affairs, Government of India and having its head office at 22, Institutional Area, Lodi Road, New Delhi. The Institute has another office at C 36, Sector – 62, Noida. ICSI is the only recognized professional body in India to develop and regulate the profession of Company Secretaries in India.

Sealed tenders are invited for **Procurement of Endpoint Protection Anti-Virus Software (Academic Version) Latest Version and Annual Onsite Comprehensive Maintenance Support** as per the details given in the Part **'A'**, **'B'** & '**C'** of the Tender Document. The terms and conditions governing the instant Tender are as under:

PART 'A'

I: Instruction to Bidders

1. The tender document may be obtained during working hours from **13th May, 2019 to 27th May**, **2019 (till 1:00 PM) on all ICSI-HQ working days on payment of Rs. 236/-(Rs. 200/- + 18% GST)** from the Reception Counter of the Institute on cash payment or by submitting a demand draft in favour of **"The Institute of Company Secretaries of India", payable at New Delhi.** The tender document can also be downloaded from the website of the Institute (www.icsi.edu) for which bidders would be required to enclose a demand draft of **Rs. 236/- (200 + 18% GST)** towards the cost of the tender document along with their quotes, failing which the tender shall be out rightly rejected. If any discrepancies found in the downloaded version of the tender, the version of the tender document kept at Purchase cell of the Institute will be treated as authentic and correct.

2. The sealed tenders are to be submitted in prescribed format on the bidder's business letter head duly stamped, signed and dated on each page of Part 'A' & 'B' and 'C' as a token of the bidder's unconditional acceptance to the terms prescribed by the Institute. Details/supporting documents wherever applicable, if attached with the tender must be

duly authenticated by the bidder. No over-writing shall be accepted unless authenticated with full signature of the bidder.

3. **Bid Submission**: Each bidder shall submit the tender in three separate sealed envelopes, (i) EMD & Tender Fee is to be put in **envelope No. 1** (please mark the envelope as **"No.1 – EMD & Tender Fee**), (ii) Part 'A' & 'B' including Form I (Annexure A), Form II(a) & II(b) (Annexure B1 & B2), and Form III (Annexure C), along with all requisite documents is to be put in **envelope No. 2** (please mark the envelope as "**No. 2 – Technical Bid**", (iii) Part 'C' only is to be put in **Envelope No. 3** (Please mark the Envelope as "**No.3 – Financial Bid**"). All the sealed envelopes bearing No. 1, 2 and 3 are to be put in main envelop i.e. Envelope No. 4.

   (Note: The bidders having valid registration with NSIC/MSME may avail exemption from submission of EMD but must enclose valid NSIC / MSME certificate/document in envelope No. 1 instead of EMD demand draft).

4. The sealed tender envelope duly super scribed, "**Procurement of Endpoint Protection Anti-Virus Software (Academic Version) Latest Version and Annual Onsite Comprehensive Maintenance Support'** due **on 27th May, 2019**" should be addressed by name to **Officiating Secretary**, ICSI and sent at the Institute's address given below either by registered post/speed post/courier or by dropping in the tender box placed at **Ground Floor** of Institute's Noida office address as mentioned below & should reach on or before **2.00 PM on 27th May, 2019**.

   Address:

   Officiating Secretary
   The Institute of Company Secretaries of India
   ICSI House, C-36, **(Ground Floor : Tender Box)**
   Sector-62 Noida – 201309 (UP)

   The Institute shall not be liable for any transit delays whatsoever and tenders received after the stipulated time/date are liable to be rejected summarily without assigning any reason and without any further reference to the bidder.

5. The **Technical Bid shall be opened on 27th May, 2019 at 3:00 PM** in the Institute of Company Secretaries of India at ICSI House, C-36, Sector-62 Noida 201309 in the presence of those bidder(s), who wish to be present. No separate communication will be sent in this regard. In the event of due date being a closed holiday or declared Holiday for ICSI-HQ / Central Government offices, the due date for opening of the bids will be the following working day at the appointed time and venue.

6. **Earnest Money Deposit (EMD)**
   i. The Earnest Money Deposit (EMD) of **Rs. 24,000/- (Rupees Twenty Four Thousand only)** in the form of Demand Draft/pay order drawn in favour of "THE INSTITUTE OF COMPANY SECRETARIES OF INDIA" payable at New Delhi only is to be submitted along

with the bid.

ii. Tenders received without the prescribed Earnest Money Deposit (EMD) shall not be entertained and shall be rejected summarily.

iii. The EMD of the successful bidder can either be converted as part of the performance security on request of the bidder or will be refunded after receipt of Performance Guarantee/Security. In case the selected bidder/vendor opts to convert the EMD to be part of the performance security, balance amount towards the performance security will be recovered from the payable amount to the vendor. The EMD of the unsuccessful bidders will be refunded without any interest/Bank commission/collection charges within 30 days after award of the contract / work order to the successful bidder.

Forfeiture Of EMD:

The EMD of the bidders shall be forfeited in the following circumstances:-

i. the bidder withdraws its bid;
ii. the selected bidder does not accept the Purchase / Work Order;
iii. the selected bidder fails to supply goods / services as per the terms of the Tender and Purchase / Work Order.
iv. any other unjustified reasons e.g. misleading or wrong information in the Bid, violation of the terms and conditions of the Tender, involvement in forming ring/cartel, submission of multiple bids in different names etc.

7. **Performance Guarantee / Security**

The successful bidder shall submit the security deposit /performance guarantee in the form of an Account payee Demand Draft / Banker's Cheque or Bank Guarantee from scheduled bank of equivalent amount of 10% of the Purchase Order on awarding the Purchase within 10 days of issue of order, to cover any loss or damage caused to or suffered by the Institute due to acts of commission and omission by the successful bidder or any failure on the part of the successful bidder in fulfillment of terms and conditions of the bid or purchase order. The Bank Guarantee shall have to remain valid for the entire duration of the Purchase Order plus three months beyond the completion of purchase order. The successful bidder shall not be entitled to any claim or receive any interest on the amount of performance guarantee. The EMD of the successful bidder will be refunded after submission of the performance Guarantee/Security Deposit.

If desired by the successful bidder in writing, the EMD may be converted into the Performance security and balance amount (if any) shall be deposited by the successful bidder with the ICSI to complete the amount of Performance Security.

8. **Forfeiture of Security Deposit and Invoking of Bank Guarantee:**

ICSI shall have the right to invoke the Bank Guarantee and to forfeit the security deposit if successful bidder contravene, withdraws or amends, impairs or derogates from Purchase Order.

ICSI shall also have the right to invoke the Bank Guarantee and to forfeit the security deposit and to adjust the damage or loss caused to the ICSI due to the negligence, carelessness, inefficiency, fraud, mischief and misappropriation or any other type of misconduct of the successful bidder or its staff / employee / agent / representative.

Whenever under Bid or Purchase Order, any sum of money is recoverable from and payable by the successful bidder, the ICSI shall have right to recover such sum by appropriating in part or in whole from the security deposit / bank guarantee of the successful bidder. In the event of the security deposit / bank guarantee being insufficient, the balance or the total sum recoverable, as may be, shall be deducted from any sum due to the successful bidder or which at any time thereafter may become due to the successful bidder. If this sum is not sufficient to cover the full amount recoverable, the successful bidder shall pay the Institute on demand the remaining amount.

9. The GST has rolled out with effect from 01.07.2017. For implementation of GST in ICSI, bidders who have not migrated to or registered with GST regime will not be able to participate in any tender of this Institute. Any offer received from the bidder without GST registration details will be summarily rejected.

10. The Bidder should not be blacklisted by Central/ State Government Ministry/ Department/ PSU/Government Company. Bidder also should not be under any legal action for indulging in corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice with any Indian Central/ State Government Ministry/Department/ PSU/ Government Company in last 5 years.

11. The Bidder is expected to examine all instructions, forms, terms and specifications in the tender / bidding documents. Failure to furnish all information required by the bidding documents may result in the rejection of its bid and will be at the bidder's own risk.

12. The bid prepared by the Bidder, as well as all correspondence and documents relating to the Bid exchanged between the Bidder and the ICSI shall be in English.

13. ICSI shall have the right to assess the competencies and capabilities of the bidder by going through the credentials given in the Technical Bid and on the basis of such credentials, ICSI may reject the candidature of the bidder without assigning any reason. In such case(s) the Financial Bid shall not be opened for that particular bidder. The Financial Bid of only those bidders shall be opened those who qualify in the technical scrutiny. Time and date for opening the financial bid shall be intimated separately through website notification at www.icsi.edu and/or email communication as furnished by the bidder in the bid document.

14. Correction and overwriting anywhere in the tender document should be avoided. Every correction and overwriting must be authenticated with full signature of the bidder, otherwise the tender is liable to be rejected.

15. ICSI reserves the right of accepting the bid in whole or in part without assigning any reason and such decision shall be final. The part acceptance of the bid shall not violate the terms

and conditions of the tender documents and the bidder shall execute the work at the specified rates without any extra charges or compensation within the stipulated period.

16. Incomplete quotations shall be rejected out rightly. No alterations, amendments or modifications shall be made by the Bidder in the Tender documents and if any such alterations are made or any special conditions attached, the bid is liable to be rejected at the discretion of the ICSI without reference to the bidder. Tempering with any format given may be liable for rejection / disqualification of the bids. Correction and overwriting anywhere in the tender document should be avoided. Every correction and overwriting must be authenticated with full signature of the bidder, otherwise the tender is liable to be rejected.

17. Each Bidder acknowledges and accepts that ICSI may in its absolute discretion apply selection criteria specified in the tender document for evaluation of proposals / bids for short listing / selecting the eligible vendor(s). All Bidders on responding to ICSI for this tender will be deemed to have accepted the terms of these tender documents. Non acceptance of any of the terms & conditions as stated in Tender document and non-submission of the stipulated Earnest Money Deposit (EMD) shall render the Bid invalid.

18. All costs and expenses incurred by Bidders in any way associated with the development, preparation, and submission of bid / responses, including but not limited to; the attendance at meetings, discussions, demonstrations, etc. and providing any additional information required by ICSI to facilitate the evaluation process, and in all such activities related to the bid process, will be borne entirely and exclusively by the bidder.

19. At any time prior to the last date for receipt of Bids, the ICSI, may, for any reason, whether at its own initiative or in response to a clarification requested by the Bidders, modify the bid / Tender documents by issuing an addendum/corrigendum. Any such amendment issued along with the original Tender document will constitute Revised Tender Documents. The addendum/corrigendum will be uploaded on the ICSI website. The Bidders are requested to visit the website frequently to check for any the decision of ICSI on the need for any modification shall be final and binding on all.

20. In order to afford prospective bidders reasonable time to take the Corrigendum into account in preparing their bids, ICSI may, at its discretion, extend the deadline for submission of bids.

21. Any Corrigendum, Clarifications etc. shall be binding on the Bidders and shall be given due consideration by them while they submit their bids.

22. The ICSI may at any time during the bidding process but before opening the technical/commercial bid request the Bidders to submit revised Technical / Commercial Bids and/or Supplementary Commercial Bids, in case of change in Scope of Work or requirement, without thereby incurring any liability to the affected Bidder(s).
23. In case of any work for which there is no specification given in the Tender document but the same is essential for the job / work mentioned in Tender document, such work shall be

carried out in accordance with the directions of the ICSI without any extra cost to the Institute.

24. This invitation for tender does not commit ICSI to award a contract / order. Further, no reimbursable cost may be incurred in anticipation of award if contract / order.

25. No binding legal relationship will exist between any of the Bidders and ICSI until issue of Purchase Order.
26. Bidder should have all necessary patents, license rights, authority, agency and other proprietary rights required in respect of any device or method used by it for completing the Purchase Order. Bidder shall indemnify and hold ICSI harmless from and against any liability, penalty, cost or expense suffered or incurred as a result of Bidder failing to comply with this obligation.
27. Prices quoted should be for Institute premises and should be inclusive of all charges, levies, octroy, taxes, fees, cess & duties and any other statutory components for **One Time cost to the ICSI except GST which is to be shown separately.**

28. **The Principal Manufacturer will provide a certificate that the Anti-virus License of Software will be in the name of the Institute. This certificate is to be submitted by the bidder with the technical bid.**

29. **Escalation Matrix up to Three (3) levels should be provided.**

30. **Penalty:** Three (3) years onsite comprehensive warranty and support for Endpoint Protection Anti-Virus for servers and nodes with 4 hours call attending support and penalty of Rs.500/- per day in case of default. After 24 hours the end user problem should be resolved within 24 hours of lodging the complaint in case of default, a penalty of Rs.500/- per day would be levied.

31. Institute's usual payment terms are 90% upon installation of Endpoint Protection Antivirus software tool and acceptance of the supplied material. The remaining 10% will be paid within thirty days of receipt of bank guarantee of equivalent amount valid for entire warranty and/or support period failing which the 10% amount will be retained during the entire period of warranty and/or support. Vendor will be fully responsible for comprehensive maintenance free of charge during the warranty and/or support period and in case of default, ICSI will have the right to arrange maintenance at vendor's risk and cost.

32. Though Institute prefers to deal with manufacturers/principal manufacturers directly, it may also consider the offers received through its authorized channel partners, provided the principal authorizes the said channel partner in this regard. **The authorization letter from the Principal Manufacturer is to be submitted with the technical bid.**

33. Delivery period of Software Licenses should be mentioned clearly in the proposal. Penalty for the late delivery and installation would be levied at the rate of:-
    (i) ½ per cent of total value of contract, for each day of delay, in case of Software Licenses are delivered within 7 days after the due date;

(ii) 1 per cent of total value of contract, for each day of delay, in case of Software Licenses are delivered beyond 7 days but upto 14 days after the due date;

(iii) 2 per cent of total value of contract, for each week of delay, in case of Software Licenses are delivered beyond 14 days subject to a maximum of 10% of total contract price

In case of delay beyond fifteen (15) days from the stipulated period, Institute may at its discretion cancel the order and arrange to procure the same from the next bidder on the panel/open market at the sole risk, cost and responsibility of the bidder.

34. In case of failure to supply the Software Licenses of the ordered quantity / specifications / quality in the time schedule and at the agreed rates in, the Institute shall have right to purchase the same from the market at the prevalent rate and the difference between the agreed price and purchase price would be recovered from the successful bidder. Further, if the supplied items are not in accordance with the ordered items then the Institute reserves the right to reject the whole lot or accept, whole or part supply, at less than the agreed / market price. Any loss to the Institute on this account shall be adjusted from the EMD / Performance Security.

I. The quantities indicated in Part –"C" is tentative and may be increased / decreased at the sole discretion of the Institute. The successful bidder shall have no right to claim any minimum / definite volume of business or enhance per unit rate.

35. **Bid Validity**: Price quoted must be valid for at least 90 days from the date of opening of bid.

36. Prices quoted should be FOR Institute premises (ICSI) Headquarters New Delhi and ICSI-Noida at Noida and should be inclusive of all charges/taxes. including installation of the Antivirus Software, and add-ons, '**acceptance test**' and charges for **Three (3) years onsite comprehensive warranty and/or support from the date of installation/purchase**. ***In case the warranty and/or support is for one year by default, the vendor shall quote for the support pack from the principal manufacturer so as to validate the warranty and/or support for Three (3) years.*** The term 'acceptance test' imply running of supplied Antivirus software for twelve hours daily for seven days including seventy-two (72) hours continuous running. If the Antivirus software fail in acceptance test the same shall be liable to be rejected. No alteration to the Antivirus software shall be permitted during the 'acceptance test'. **The principal Manufacturer will provide a certificate of warranty and/or support for Three (3) years.**

37. **Bid Evaluation**:
ICSI shall have the right to assess the competencies and capabilities of the Tenderer by going through the credentials given in the Technical Bid and on the basis of such credentials, ICSI may reject the candidature of the Tenderer without assigning any reason. In such case(s) the Financial Bid shall not be opened for that particular Tenderer. The Financial Bid of only those parties who qualify in the technical scrutiny shall be opened and time and date for opening the financial bid shall be intimated separately.

38. The Institute reserves the right to accept or reject any or all the tenders including the lowest tender(s) without assigning any reason at its sole discretion and the decision of the Institute will be final and binding on all concerned. The Institute also reserves its rights to cancel the whole tender process at any stage without assigning any reason whatsoever.

39. **Eligibility Criteria**

a. Average of the turnover of last three Financial Years (i.e. 2017 – 2018, 2016 – 2017, 2015 – 2016) collectively should not be less than Rs.40.00 lakhs.(Please attach copy of Audited P&L accounts and balance sheet of three preceding consecutive financial years ending as on 31st March, 2018 of the bidding firm in support of the bidder's submission).

b. The Principal Manufacturer will provide a certificate of Anti-virus Software License will be in the name of the Institute. This certificate is to be submitted by the bidder with the technical bid.

c. The authorization letter/Certificate from the Principal Manufacturer as an Authorized Dealer/Partner.

d. The bidder should be Authorized Reseller/partner for past Three (3) years for the proposed OEM/Product.

e. Bidders must have GST registration and PAN. (Please attach self-attested photocopy of the documents).

f. The bidder must have a valid as on the date of submission of the bid ISO 9001:2008 / Equivalent certificate for quality (OR) ISO 20000-1:2011 / Equivalent certificate for Data Security. (Please attach supporting document)

g. The bidder must have their own Office set up in Delhi/NCR and they should have technical manpower availability to assist at ICSI Site as and when required to extend technical support on site.

h. The firm having at least 3 year experience in the field of Anti-Virus sales and Technical Support with 5 AMC/sales work orders out of which 3 orders of minimum value of Rs.10.00 Lakh each from any Government / MNC firm. The bidder must have a satisfactory performance certificate regarding AMC/sales from similar works from client/customer. (Please attach self-attested photocopy of the documents)

The bidder must comply the above mention eligibility conditions, if any bidder not fulfills the same, they will be technically rejected.

III: General Terms and conditions

1. The Contract shall be for a period of Three (03) years. However, Institute at its discretion, can terminate the contract without citing any reason at any point of time by giving three (03) months' notice. In case of termination, Institute will be liable to pay pro-rate amount to the vendor only for the period for which the Anti-virus services availed by the Institute. Contract may be extended for a further period of one year on the same rates, terms and conditions as mutually agreed upon.

2. The successful bidder has to submit the security deposit /performance guarantee from scheduled bank of equivalent amount of 10% of the contract value on awarding the contract within 10 days of issue of order but before execution of the agreement, to cover any loss or damage caused to or suffered by the Institute due to acts of commission and omission by the successful bidder or any failure on the part of the successful bidder in fulfillment of terms and conditions of the contract and conditions contained in the agreement. The Bank Guarantee shall have to remain valid for the entire duration of the Contract plus three months beyond the completion of contract period. The successful bidder shall not be entitled to any claim or receive any interest on the amount of performance guarantee. The EMD of the successful bidder will be refunded after submission of the performance Guarantee/Security Deposit.

   The successful bidder having valid registration with NSIC/MSME on the date of submission of tender, are also required to submit requisite security deposit / performance guarantee.

3. Kindly submit duly filled in and signed Declaration & Acceptance of Terms and Conditions, as per Performa enclosed in **Annexure – C**

4. The quantities indicated in Part –"C" is tentative and may be increased/decreased at the sole discretion of the Institute and the vendor shall have no right to claim any minimum/definite volume of business.

5. Secretary of the Institute reserves the right to accept or reject any or all tender/s received and such decision shall be final.

6. General:

(a) Law, governance and jurisdiction:

i. **Dispute Resolution:** Any dispute, difference, controversy or claim ("Dispute") arising between the successful bidder and ICSI hereinafter jointly to be called "parties" and singularly as "party" out of or in relation to or in connection with the contract, or the breach, termination, effect, validity, interpretation or application of this contract or as to their rights, duties or liabilities hereunder, shall be addressed for mutual resolution by the authorized official of the parties. If, for any reason, such dispute cannot be resolved amicably by the Parties, the same shall be

referred to the Sole Arbitrator who would be the Secretary of the Institute of Company Secretaries of India or any other person appointed by him as Sole Arbitrator. The provisions of the Arbitration and Conciliation Act, 1996 or any statutory modifications on re-enactment thereof as in force will be applicable to the arbitration proceedings. The venue of the arbitration shall be at New Delhi. The cost of the Arbitration proceedings shall be shared equally by both the parties. The language of the arbitration and the award shall be English. The decision / award of the arbitrator shall be final and binding on parties to the arbitration proceedings.

ii. **Law:** This Tender shall be governed in accordance with the laws of Republic of India. These provisions shall survive the Contract

iii. **Jurisdiction:** The courts of India at Delhi have exclusive jurisdiction to determine any proceeding in relation to this Tender. These provisions shall survive the Contract.

(b) CONFIDENTIALITY: The successful bidder acknowledges that all material and information which has and will come into its possession or knowledge in connection with this agreement or the performance thereof, whether consisting of confidential and proprietary data or not, whose disclosure to or use by third parties may be damaging or cause loss to ICSI will all times be held by it in strictest confidence and it shall not make use thereof other than for the performance of this agreement and to release it only to employees requiring such information, and not to release or disclose it to any other party. The successful bidder agrees to take appropriate action with respect to its employees to ensure that the obligations of non-use and non-disclosure of confidential information under this agreement are fully satisfied. In the event of any loss to ICSI in divulging the information by the employees of the successful bidder, the ICSI shall be indemnified. The successful bidder agrees to maintain the confidentiality of the ICSI's information after the termination of the contract also. The successful bidder will treat as confidential all data and information about the ICSI /Contract, obtained in the execution of this tender including any business, technical or financial information, in strict confidence and will not reveal such information to any other party.

(c) Dispute Resolution: Any dispute, difference, controversy or claim ("Dispute") arising between the bidder and ICSI hereinafter jointly to be called "parties" and singularly as "party" out of or in relation to or in connection with the bidding, purchase order , or the breach, termination, effect, validity, interpretation or application of this Tender/bid or purchase order or as to their rights, duties or liabilities hereunder, shall be addressed for mutual resolution by the authorized official of the parties. If,

for any reason, such dispute cannot be resolved amicably by the Parties, the same shall be referred to the Sole Arbitrator who would be the Secretary of the Institute of Company Secretaries of India or any other person appointed by him as Sole Arbitrator. The provisions of the Arbitration and Conciliation Act, 1996 or any statutory modifications on re-enactment thereof as in force will be applicable to the arbitration proceedings. The venue of the arbitration shall be at New Delhi. The cost of the Arbitration proceedings shall be shared equally by both the parties. The language of the arbitration and the award shall be English. The decision / award of the arbitrator shall be final and binding on parties to the arbitration proceedings.

(d) **SUB-CONTRACTING:** The successful bidder will not assign or transfer and sub-contract its interest / obligations under this contract to any other concern / individual without the prior written consent of the ICSI.

Statutory Compliance: The successful bidder will be required to comply with all statutory obligations from time to time applicable to this contract.

(e) **Force Majeure**

i) For the purpose of this Article, Force "Majeure" means any cause, which is beyond the successful bidder control or that of the Institute, as the case may be, which both could not foresee or with a reasonable amount of diligence could not have foreseen, and which substantially affect the performance of the order, such as:-

- War / hostilities

- Riot or civil commotion

- Earth Quake, Flood, Fire, Tempest, Epidemics, Lightning or other natural physical Disaster, Quarantine restricts and Freight embargoes

- Restrictions imposed by the Government or other statutory bodies, which is beyond the successful bidder control or of the Institute, which prevent or delay the execution of the order either by the successful bidder or by the Institute.

ii) If a Force Majeure situation arises, the successful bidder are required to promptly notify ICSI in writing of such condition and the cause thereof within a period of three (3) days from the date of happening of such an event requiring invocation of this force majeure article. Unless otherwise directed by the ICSI in writing, the successful bidder will continue to perform its obligations under this order as far as is reasonably practical and shall seek all reasonable alternative means for performances of this order.

(f) **Indemnity Clause:** The successful bidder will indemnify ICSI against all statutory liabilities present and future arising out of this contract. In the event of violation of any contractual or statutory obligations, the successful bidder will be fully and solely

responsible for the same. Further, in the event of any action, claim, damages, suit initiated against ICSI by any individual, law enforcement agency or government authority due to acts and omissions, the successful bidder will be liable to make good/compensate such claims or damages to the ICSI. As a result of the successful bidder action, inaction or any omissions, if ICSI is required to pay any damages to any individual, law enforcement agency or government authority, the successful bidder would be required to reimburse to ICSI such amount along with other expenses incurred by ICSI or ICSI reserves the right to recover but not limited to such amount from the payment(s) due to the successful bidder while settling its bills or from the amount of security deposit lying with ICSI. However, ICSI reserves its right to take legal recourse as permitted under law of the land.

(g) Black-Listing – Bidder would be liable to be black-listed under following circumstances:-

- Giving false, misleading or fake information / document in the bid;
- Withdrawing the bid after opening of the Financial bids;
- Refusal to accept Purchase Order at the quoted prices;
- Failure to supply goods of the ordered quantity / quality / specifications at the agreed rates within the time schedule;
- Adoption of any unethical or illegal practices;
- Any other justified reason.

EMD of black-listed Bidder shall be forfeited after giving him an opportunity of being heard. The decision of the ICSI shall be the final and binding.

(h) Cancellation of Award / Purchase Order: The ICSI without prejudice to any other remedy, reserves the right to cancel the Award / Purchase Order in whole or in part by giving one (1) months' notice in writing in case the successful bidder fails to discharge its obligation under this tender / Purchase Order without sufficient ground or found guilty for breach of condition(s) of this tender / Purchase Order, negligence, carelessness, inefficiency, fraud, mischief and misappropriation or due to any other type of misconduct by the successful bidder or by its staff or agent.

Any pending or unresolved operational issues, performance, unpaid fees and any other remedies shall be continued by the successful bidder during the period of the termination notice and the same must be satisfied / completed before the Purchase order is cancelled. The ICSI may also put in place any other agency for carrying out the remaining work and expenditure incurred on same shall be recovered from the successful bidder.

(i) Jurisdiction of Courts: All disputes arising out of or relating to the tendering / bidding and Purchase order shall be deemed to have arisen in New Delhi and only courts having jurisdiction over Delhi shall determine the same.

(j) TERMINATION: The ICSI without prejudice to any other remedy, reserves the right to terminate the agreement in whole or in part by giving Three (3) months' notice in writing in case the successful bidder fails to discharge its obligation under this agreement/contract without sufficient ground or found guilty for breach of condition(s) of the agreement, negligence, carelessness, inefficiency, fraud, mischief and misappropriation or due to any other type of misconduct by the successful bidder or by its staff or agent.

Any pending or unresolved operational issues, performance, unpaid fees and any other remedies shall be continued by the successful bidder during the period of the termination notice and the same must be satisfied / completed before this agreement/contract is terminated. The ICSI may also put in place any other agency for carrying out the remaining work and expenditure incurred on same shall be recovered from the successful bidder.

For any further details/clarifications, Dr. Nikhat Khan, Director, IT may be contacted (0120-4522019), E-mail- Nikhat.khan@icsi.edu

Date: 13th May, 2019

(Amit Kumar Ghosal)
DIRECTOR (Purchase & Stores)

(Annexure A)

THE INSTITUTE OF COMPANY SECRETARIES OF INDIA
ICSI HOUSE, C-36, SECTOR-62, NOIDA -201309

Tender No: PC/IT/Anti-Virus/2019 **13th May, 2019**

Sub: Procurement of Endpoint Protection Anti-Virus Software (Academic Version) Latest Version and Annual Onsite Comprehensive Maintenance Support.

PART 'B' (TECHNICAL BID)

Form I: PARTICULARS OF BIDDER

(ALL COLUMNS ARE TO BE FILLED IN BLOCK LETTERS)

1. Name of the bidder

(a) Trade Name _____

(b) Status of the Bidder _____

(Limited Co./ LLP /Partnership/ Proprietorship)

(Enclose self attested copy of document)

(c) Name of CEO/Directors /Partners/ Proprietor _____

2. Postal Address _____

_____

3. Telephone No. / Mobile No. for communication _____

4. (a) E-mail-id (mandatory)
(b) Website address (if available) _____

5. Bank Draft No, date, Bank name and amount (if applicable)/MSME or NSIC Regn. No.
(a) Tender Fees _____
(b) EMD _____
(c) MSME/NSIC Regn. No. (if applicable) & its valid period _____
(Enclose self-attested certificate photocopy)

6. Name of the Banker, Branch Name, A/c No. and IFS Code
(for e-payment purpose) _____

7. PAN (Enclose self-attested photocopy) _____

8. GSTIN Code (Enclose self-attested photocopy) _____

9. Lab. Licence/EPF/ESIC Reg. No. (if applicable) _____

(Enclose self-attested photocopy)

10. Please also specify, if bidder is registered with appropriate Authority under Works Contract Act, 1999. _____
(Enclose self-attested photocopy)

11. Trade License/Business License/CIN (if applicable) _____
(Enclose self-attested photocopy)

I/We hereby declare and affirm that I/we have read and understood the terms and conditions of this tender/quotation/NIT as stipulated in the tender notice No._____. Accordingly, I/ we accept the terms and conditions and hereby offer the rates for "_____(name of the work or supply)" as per Financial Bid (Part 'C').

Signature _____
(Authorized signatory of the agency)
Name of the bidder_____
Date_____ **Official seal of bidder** _____

- **NOTE: Please submit all supporting documents (self-attested photocopy) wherever applicable in support of the information furnished above with seal and signature of the bidder's authorized representative.**

(Annexure B1)

THE INSTITUTE OF COMPANY SECRETARIES OF INDIA
ICSI HOUSE, C-36, SECTOR-62, NOIDA -201309

Tender No: PC/IT/Anti-Virus/2019 **13th May, 2019**

Sub: Procurement of Endpoint Protection Anti-Virus Software (Academic Version) Latest Version and Annual Onsite Comprehensive Maintenance Support.

Form II(a): TECHNICAL DETAILS

Sl.No.	Particulars.	Response
1	List of existing clients to whom Anti-Virus Software tool maintenance service under AMC has been provided in last 1 year with details of company, value of business, concerned person name & his telephone no. (Please attach full details)	
2	A) List of existing sites being maintained as per following: Name of the Company/Type of Software being maintained/No./Last Year's turn over. B) Please indicate the Software principal/s brands you represent and your level of association	
3	Please indicate in full the following details: A) Manpower available – Technical & Non-technical Number and name of the personnel who can provide Anti-virus Software tool support and do trouble shooting. B) Turnover of the company for last 3 financial years (2014-15, 2016-17 & 2017-18). (Please attach supporting documents)	
4	Paid up capital of the firm.	
	Authorization letter/Certificate from Microsoft (OEM) as an Authorized Dealer/Partner.	

Date:

Signature _____
(Authorized signatory of the agency)
Name of the bidder_____

Technical Specification of Advance Endpoint Protection Anti-Virus tool

General requirements:	**compliance Yes/No**	**Remarks**
Antivirus protection solution should consist of:		
• OEM should be present in Gartner quadrant for any of last three consecutive years in last 5 years for endpoint security. (OR) OEM should be "Top Player" in Radicati quardent for endpoint security.		
• Antivirus protection software for Windows desktops.		
• Antivirus protection software for Windows File Servers.		
• Antivirus protection software for Linux File Servers.		
• Antivirus protection software for MAC		
• Antivirus protection software for Windows Terminal Servers.		
• Centralized management, monitoring and update software		
• Antivirus bases signatures of malicious software and cyber-attacks.		
• Documentation.		
Antivirus protection for Windows desktops:		
Antivirus protection software for Windows desktops should be running on the following operating systems:		
• Microsoft Windows XP Professional SP3 x86 and higher;		
• Microsoft Windows Vista SP2 x86 /x64 and higher;		
• Microsoft Windows 7 Professional / Enterprise /Ultimate x86 / x64;		
• Microsoft Windows 7 Professional / Enterprise /Ultimate SP1 x86 / x64 and higher;		
• Microsoft Windows 8 Professional / Enterprise x86 / x64;		
• Microsoft Windows 8.1 Professional / Enterprise x86 / x64;		
• Microsoft Windows 10 Pro / Enterprise x86 / x64;		
• Microsoft Windows Embedded Standard 7 SP1 x86 / x64;		
• Microsoft Windows Embedded POS Ready 7 x86 / x64;		
• Microsoft Windows Embedded 8.0 Standard x64;		
• Microsoft Windows Embedded 8.1 Industry Pro x64.		
Antivirus protection software for Windows desktops should have the following functionality:		
• Real-time and on-demand antivirus scan.		
• Heuristic analyzer for detection and blocking of unknown (zero days) malware.		
• Schedule-based antivirus scanning.		
• Ability to run product specific tasks by schedule or just after OS boot.		
• Ability to scan and cure files packed in RAR, ARJ, ZIP, CAB archives, including password protected archives.		
• Cloud protection from new threats allowing product to perform cloud requests in real-time during on-access and on-demand scans to get actual verdict in regards to the object.		
• Mail threats protection with ability to scan incoming and outgoing mail flows delivered via the following protocols: IMAP, SMTP, POP3, MAPI, NNTP — regardless of mail client software vendor used by end user;		
• Web traffic protection with ability to scan objects delivered to end user computer via HTTP and FTP protocols, including possibilities to perform heuristic analysis and define trusted sites excluded from the scan.		
• Ad banners and pop-up windows block.		
• Detection and block access to phishing links.		
• Ability to detect anomalies in application behaviour. Ability to roll back all actions done by a malware, including recovery of files encrypted by a malware.		

• Ability to limit privileges of running applications, including registry modification and file access, in automated way based on application reputation.		
• Protection from attacks like Bad USB.		
• Network monitor with ability to set up per application network rules for certain protocols (TCP, UDP) and ports.		
• Network attacks protection by leveraging on IDS/IPS components based on rules of most popular applications activities working within any type of networks, including wireless.		
• Ability to define rules preventing installation and start-up of any given application via controlling of applications by their OS path, metadata, file hashes and predefined categories supplied by ISV with possibility to define exclusion within these rules for certain Active Directory user accounts.		
• Ability to control user activities with external I/O devices by device type, bus type, device identifier and vendor. There is also should be a possibility to define list of trusted devices based on device ID and allow certain Active Directory users to gain access to these devices in default deny mode.		
• Ability to control Web surfing, including possibility to deny or allow access to certain web resources and data types (e.g. audio, video, etc.), with possibility to tie rules by time and any given Active Directory user.		
• Reduced scan time by omitting scan of unchanged objects since last scan.		
• Ability to find vulnerabilities within installed applications with possibility to get the report of all found vulnerabilities.		
• Flexible resource utilization of antivirus software allowing decreasing impact on end user experience during file scan to minimum.		
• Self-defence functionality preventing unauthorized users and malware applications modify antivirus software settings and disable antivirus protection.		
• Ability to install custom set of protection components.		
• Solution should have an Application provisioning feature E.g. Administrator can deploy third party software on command or can schedule it for outside normal office hours. The software deployment process should be entirely transparent to users.		
• Solution should have a License Provisioning and Control feature (E.g. centralised licence provisioning and tracking of any breaches of licence conditions)		
• Solution should have Asset management feature – hardware & software (E.g. all devices and software on the network should be automatically discovered and recorded in hardware and software inventories.)		
• Solution should have Patch Management features - Advanced in-depth scanning for vulnerabilities combined with the automated distribution of patches.		
• Solution should have a Remote troubleshooting and deployment tool I.e. it should help administrator to resolve problems efficiently. Furthermore, when he needs to deploy new software at a remote office, he can reduce the load on his network by using one local workstation as the update agent for the whole site.		
• Solution should have option to integrate with SIEM systems like, HP ArcSight & IBM QRadar		
• Solution should have full-disk, file level & removable media backed by Advanced Encryption Standard (AES) with 256 bit encryption to secure critical business information in the event of device theft or loss.		
• Full Disk Encryption should operate on the physical sectors of the disk – to deliver encryption that's 'close to the hardware' and also enable an 'encrypt everything at once' strategy.		
• File level Encryption should offer granular encryption of individual files and helps to enable secure sharing of data across your network.		
• Solution should have a feature to Increase security through policies that enforce the encryption of data on removable devices.		
• Solution should support Portable Mode for File Level Encryption on removable media		

• Users can create password-protected, encrypted, self-extracting packages of files and folders. This enables the secure transfer and sharing of sensitive data – via a removable device, email or the web.		
• Administrator should be able to access vital encrypted data in the event of a system failure – even if the operating system is unable to boot.		
• If a user loses or forgets their password, a challenge / response mechanism should allow the recovery of the pre-boot password to access the encrypted data		
• Centralized management of all protection components available in antivirus protection software.		
Antivirus protection for Windows File Servers:		
Antivirus protection software for Windows File Servers should be running on the following operating systems:		
• Microsoft Windows Server 2008 Standard/Enterprise SP2 x32/x64;		
• Microsoft Windows Server 2008 R2 x64 Standard/Enterprise;		
• Microsoft Windows Server 2008 R2 x64 Standard/Enterprise SP1;		
• Microsoft Windows Server 2012 Foundation x64;		
• Microsoft Windows Server 2012 Standard x64;		
• Microsoft Windows Server 2012 R2 Standard x64 Edition.		
• Microsoft Windows Server 2016 Essentials / Standard / Data centre / Core		
• Microsoft Windows Storage Server 2016		
• Microsoft Windows Hyper-V Server 2016		
Antivirus protection software for Windows File Servers should have the following functionality:		
• Real-time and on-demand antivirus scan.		
• Traffic Security to protect your servers from web threats sent via HTTP or HTTPS traffic, and from other email-based threats.		
• Device Control to allow or block file transfers with external data storage devices (USB and MTP storage devices, CD/DVD devices).		
• Exploit Prevention to protect processes from exploits using distributed mitigation techniques.		
• Diagnostic Interface to control the server protection status, review important application status markers and manage the trace and dump files settings without installing the Administration Tools.		
• Ability to track USB connections to protected devices		
• Firewall Management to manage Windows Firewall rules through the graphical user interface.		
• Anti-Cryptor functionality to protect from Ransomware/Encryption malwares.		
• Antivirus scan initiated by end user or administrator manually and by schedule.		
• Ability to run product specific tasks by schedule or just after OS boot.		
• Cloud protection from new threats allowing product to perform cloud requests in real-time during on-access and on-demand scans to get actual verdict in regards to the object.		
• Network monitor with ability to set up per application network rules for certain protocols (TCP, UDP) and ports.		
• Network attacks protection by leveraging on IDS/IPS components based on rules of most popular applications activities working within any type of networks, including wireless.		
• Ability to find vulnerabilities within installed applications with possibility to get the report of all found vulnerabilities.		
• Ability to scan and cure files packed in RAR, ARJ, ZIP, CAB archives, including password protected archives.		
• Reduced scan time by omitting scan of unchanged objects since last scan.		
• Ability to configure dedicated scan task for critical parts of server OS.		

• Control of distribution resource utilization between antivirus software and server applications based on task priority. Possibility to continue scan in background.		
• Notify administrator about important events related to antivirus protection by mail, sound, pop-up window and log record.		
• Self-defence functionality preventing unauthorized users and malware applications modify antivirus software settings and disable antivirus protection.		
• Centralized management of all protection components available in antivirus protection software.		
Antivirus protection for Linux File Servers:		
Antivirus protection software for Linux File Servers should be running on the following operating systems:		
• Red Hat Enterprise Linux 6.5, 6.6, 6.7, 7.2 x32/x64;		
• CentOS 6.5, 6.6, 6.7 x32/x64;		
• CentOS 7.2 x64;		
• SUSE Linux Enterprise Server 11 SP3/SP4 x32/x64;		
• SUSE Linux Enterprise Server 12 x64;		
• SUSE Linux Enterprise Server 12 SP1 x64;		
• Novel Open Enterprise Server 11 SP2 x64;		
• Novel Open Enterprise Server 2015;		
• Ubuntu Server 12.04.5 LTS x32/x64;		
• Ubuntu Server 14.04 LTS x32/x64;		
• Ubuntu Server 15.10 LTS x32/x64;		
• Oracle Linux 7.2 x64;		
• Debian GNU/Linux 7.9/8.2 x32/x64;		
• OpenSuse 13.1 x32/x64;		
• OpenSuse 13.2 x32/x64;		
• OpenSuse LEAP 42.1 x64;		
• GosLinux 6.6 x32/x64;		
• Linux Mint 17.3 x64.		
Antivirus protection software for Linux File Servers should have the following functionality:		
• Real-time resident antivirus protection of defined filesystem regions.		
• Antivirus scan initiated by end user or administrator manually and by schedule.		
• Scan file systems mounted via SMB/ CIFS/ NFS protocols		
• Antivirus scan and cure of archived files.		
• Ability to run product specific tasks by schedule or just after OS boot.		
• Ability to quarantine suspicious and infected objects.		
• Provide reports in HTML, CSV, PDF and XLS.		
• Ability to intercept and scan file IO on SMB mounted filesystems.		
• Ability to backup scanned object in reserved storage and restore it back after curing or deletion in case of false positives.		
• Remote management and configuration via web browser.		
• Centralized management of all protection components available in antivirus protection software.		
Antivirus protection for dedicated server roles, including Windows Terminal Servers:		
Antivirus protection software for dedicated server roles, including Windows Terminal Servers should be running on the following operating systems:		
• Microsoft Windows Server 2008 Core/Standard/ Enterprise / Datacentre SP1 and higher;		
• Microsoft Windows Server 2008 R2 Core/ Standard/ Enterprise / Datacentre SP1 and higher;		
• Microsoft Windows Server 2012 Core/Standard/ Essential/ Datacentre/Foundation;		
• Microsoft Windows Server 2012 R2 Core/Standard/ Essential/		

Datacentre/Foundation;		
• Microsoft Windows Server 2016 TP4;		
• Microsoft Windows Storage Server 2008 R2;		
• Microsoft Windows Storage Server 2008 R2 SP2 Standard Edition;		
• Microsoft Windows Storage Server 2008 R2 SP2 Workgroup Edition;		
• Microsoft Windows Storage Server 2012;		
• Microsoft Windows Storage Server 2012 R2;		
• Microsoft Windows Hyper-V Server 2012;		
• Microsoft Windows Hyper-V Server 2012 R2.		
Terminal servers:		
• Microsoft Terminal Services based on Windows Server 2008;		
• Microsoft Terminal Services based on Windows Server 2012;		
• Microsoft Terminal Services based on Windows Server 2012 R2;		
• Microsoft Terminal Services based on Windows Server 2016;		
• (Optional) Citrix XenApp 6.0/6.5/7.0/7.5/7.6;		
• (Optional) Citrix Xen Desktop 7.0/7.1/7.5/7.6.		
Antivirus protection software dedicated server roles, including Windows Terminal Servers should have the following functionality:		
• Antivirus scan for dedicated server roles, including Terminal servers, Print servers, Application servers, File servers, Web servers and Domain controllers.		
• Antivirus protection of servers incorporated in Windows clusters.		
• On access/modification antivirus scan of the following objects: files, alternate NTFS streams, MBR and boot sectors of local and removable drives.		
• Prevent virus sprawl by virus attacks detection.		
• Recovery after infection by removing all malware related artifacts, including system files, registry and hence to prevent possible OS faults and crashes.		
• Cloud protection from new threats allowing product to perform cloud requests in real-time during on-access and on-demand scans to get actual verdict in regards to the object.		
• Real-time monitoring of VBScript and Jscript execution, created by using of Microsoft Windows Script Technologies (and Active Scripting). Script code execution scanning and preventing execution of dangerous scripts.		
• Ability to block remote access to network resources of the protected server.		
• Monitoring/prevention of attempts to encrypt files located in shared folders on the protected server as well as blocking of remote computers acting as a source of such attempts.		
• On-demand full scan.		
• Integrity control of own application modules.		
• Ability to quarantine suspicious and infected objects and restore them on shared folders.		
• Antivirus protection for terminal servers working in desktop/applications publishing modes.		
• Scalability and performance gain on multi-processor servers through defining the amount of working antivirus processes.		
• Control of distribution resource utilization between antivirus software and server applications based on task priority. Possibility to continue scan in background.		
• Ability to define trusted processes which can be somehow affected by antivirus (e.g. backup software, low latency software, etc.)		
• Local management console with possibility to connect to remote servers for their management.		
• Role-based access control for protection management/configuration based on standard Microsoft Windows facilities.		
• Default exclusions for dedicated server roles (domain controllers, SQL server, etc.).		

• Notify administrator about important events related to antivirus protection by mail, sound, pop-up window and log record. Simple Network Management Protocol (SNMP) support.		
• Support antivirus protection for data located on top of ReFS (Resilient file system) and CSV (Cluster Shared Volume) volumes.		
• Centralized management of all protection components available in antivirus protection software.		
Centralized management, monitoring and update software facilities:		
Centralized management, monitoring and update facilities should be running on the following operating systems:		
• Microsoft Windows 7 Professional/Enterprise/Ultimate x86 / x64;		
• Microsoft Windows 8 Professional / Enterprise x86 / x64;		
• Microsoft Windows 8.1 Professional / Enterprise x86 / x64;		
• Microsoft Windows 10 x86 / x64;		
• Microsoft Windows Server 2008 x86 / x64;		
• Microsoft Windows Server 2008 R2;		
• Microsoft Windows Server 2012;		
• Microsoft Windows Server 2012 R2;		
• Microsoft Windows Small Business Server 2008;		
• Microsoft Windows Small Business Server 2011.		
Centralized management, monitoring and update software facilities should be compatible with the following RDBMS:		
• Microsoft SQL Express 2005/2008/2008R2/2012/2014;		
• Microsoft SQL Server 2005/2008/2008R2/2012/2014;		
• Microsoft Azure SQL Database;		
• MySQL 5.0.67, 5.0.77, 5.0.85, 5.0.87(SP1), 5.0.91;		
• MySQL Enterprise 5.0.60(SP1), 5.0.70, 5.0.82(SP1), 5.0.90.		
Centralized management, monitoring and update software facilities should be running on the following virtual platforms:		
• VMware Workstation 9.x, Workstation 10.x;		
• VMware vSphere 5.5; Workstation 6;		
• Microsoft Hyper-V: 2008, 2008 R2, 2012, 20012 R2;		
• Microsoft Virtual PC 2007;		
• Parallels Desktop 7 and higher;		
• (Optional) Citrix Xen Server 6.1, 6.2;		
• Oracle VM Virtual Box 4.0.4-70112.		
Centralized management, monitoring and update software facilities should have the following functionality:		
• Deployment of antivirus protection management software from a single place/distributive.		
• Deployment of antivirus protection management software based on protected network size (#nodes).		
• Ability to get information about protected computers and user accounts from Active Directory.		
• Ability to discover unprotected computers within corporate network by IP, hostname, domain name and subnet mask.		
• Automatic distribution of managed computers between managed groups with possibility to define rules for auto placement for newly discovered hosts based on IP, OS type and OU in Active Directory.		
• Centralized deployment and update of antivirus protection software. Centralized configuration, administration and reporting of deployed antivirus protection software.		
• Centralized uninstall of applications incompatible with antivirus protection software.		

• Possibility to deploy antivirus protection agents in various ways: remotely via RPC, GPO, locally. Possibility to create standalone customized package of antivirus protection software.		
• Ability to define certain triggers (and hierarchy of them) in protection policy that can redefine protection settings for the given host based on logged on user account, ip address, belonging to the given computer/user OU or managed group.		
• Automatic vulnerability scan of OS and installed applications.		
• Quality assurance of all software updates designated for the given managed host/application before their deployment in production environment.		
• Ability to discover virtual machines within protected environment and optimal antivirus software configuration based on that.		
• Ability to deploy multi-tier management system with role-based access control for protection management/configuration with reporting facilities on each management layer.		
• Ability to create hierarchy of management servers with any nesting level and possibility to manage all hierarchy levels from the top.		
• Multi-tenancy support.		
• Ability to update application modules and antivirus bases from different sources and by various means, including network and local data sources.		
• All access to ISV cloud during scan is performed via centralized management server.		
• Automatic license provisioning on managed hosts.		
• Software and hardware inventory on managed hosts.		
• Ability notifies administrators about antivirus software events with possibility to configure such notifications.		
• Mobile device management via Exchange ActiveSync.		
• Mobile device management via iOS MDM.		
• SMS alerts for pre-defined events.		
• Decrease impact on protected network by distribution of antivirus updates via dedicated hosts existing in each network segment, so that all hosts in the segment get the updates from it rather than from management server.		
• Decrease impact on protected network by consolidating antivirus software events via dedicated hosts existing in each network segment, so that all hosts in the segment send events to dedicated hosts where they are aggregated and sent to management server.		
• Graphical reports based on antivirus events, hardware and software inventory, etc.		
• Predefined report templates.		
• Reports export into PDF, XML & HTML		
• Centralized management of all objects placed in quarantine and reserved storage.		
• Ability to define local user accounts on management server for management purposes.		
• Native backup facilities for management server and its database.		
• Windows Failover Clustering support.		
• Windows Certificate Authority integration.		
• Web-based management console.		
Antivirus bases update:		
Antivirus bases update process should provide the following possibilities:		
• Periodic update by schedule.		
• Ability to update application modules and antivirus bases from different sources and by various means, including network and local data sources.		
• Integrity control of antivirus bases via digital signatures.		
Documentation requirements:		
Antivirus software should have appropriate documentation, including:		
• User/administrator guide		

• Documentation should explain in details the process of antivirus software deployment, configuration and usage.		
• Antivirus software should have context help.		
Technical support requirements:		
Technical support implies:		
• Technical support provided by certified professional from ISV side or its partners via telephone, mail and web channels.		
• ISV web site of antivirus software should have appropriate sections related to the given antivirus software, including support knowledge bases and community forum.		

(Annexure B2)

THE INSTITUTE OF COMPANY SECRETARIES OF INDIA
ICSI HOUSE, C-36, SECTOR-62, NOIDA -201309

Tender No: PC/IT/Anti-Virus/2019 **13th May, 2019**

Sub: Procurement of Endpoint Protection Anti-Virus Software (Academic Version) Latest Version and Annual Onsite Comprehensive Maintenance Support.

Form II(b): Eligibility Criteria Details

S. No.	Particulars	Response Yes/No	Supporting Document Reference with Page No.
a)	Average of the turnover of last three Financial Years (i.e. 2017 – 2018, 2016 – 2017, 2015 – 2016) collectively should not be less than Rs.40.00 lakhs.(Please attach copy of Audited P&L accounts and balance sheet of three preceding consecutive financial years ending as on 31st March, 2018 of the bidding firm in support of the bidder's submission).		
b)	The Principal Manufacturer will provide a certificate of Anti-virus Software License will be in the name of the Institute. This certificate is to be submitted by the bidder with the technical bid.		
c)	The authorization letter/Certificate from the Principal Manufacturer as an Authorized Dealer/Partner.		
d)	The bidder should be Authorized Reseller/partner for past Three (3) years for the proposed OEM/Product.		
e)	Bidders must have GST registration and PAN. (Please attach self-attested photocopy of the documents).		
f)	The bidder must have a valid as on the date of submission of the bid ISO 9001:2008 / Equivalent certificate for quality (OR) ISO 20000-1:2011 / Equivalent certificate for Data Security. (Please attach supporting document)		
g)	The bidder must have their own Office set up in Delhi/NCR and they should have technical manpower availability to assist at ICSI Site as and when required to extend technical support on site.		
h)	The firm having at least 3 year experience in the field of Anti-Virus sales and Technical Support with 5 AMC/sales work orders out of which 3 orders of minimum value of Rs.10.00 Lakh each from any Government / MNC firm. The bidder must have a satisfactory performance certificate		

	regarding AMC/sales from similar works from client/customer. (Please attach self-attested photocopy of the documents)		

The bidder must comply the above mentioned eligibility conditions and if any bidder does not fulfill the same, they will be technically rejected.

Date:

Signature _____
(Authorized signatory of the agency)
Name of the bidder_____

(Annexure C)

Form III: Tender acceptance letter to be printed on business letterhead of the bidder and to be submitted with the Technical Bid

To
The Secretary
Institute of Company Secretaries of India (ICSI)
ICSI House,
C – 36,
Sector 62,
Noida-201309

Sub: Procurement of Endpoint Protection Anti-Virus Software (Academic Version) Latest Version and Annual Onsite Comprehensive Maintenance Support.

Sir,

This is with reference to the **Tender No: PC/IT/Anti-Virus/2019** due on **_____.** We are interested to participate in the **Tender for Procurement of Endpoint Protection Anti-Virus Software (Academic Version) Latest Version and Annual Onsite Comprehensive Maintenance Support _____, 2019.** We declare that:

i) We have read and understood the terms and conditions given in the quotation / tender Document;

ii) We are eligible for award of the contract as per the qualification criteria mentioned in the quotation / tender Document;

iii) We accept and agree to all the terms and conditions of the quotation / tender;

iv) We shall comply with all the terms and conditions of the quotation / tender;

v) All the information / documents provided in this bid are true to the best of our knowledge and belief. If at any stage, the information / documents are found to be false, misleading or incorrect then this Bid / Purchase Order shall be cancelled at our cost and risk and we shall indemnify the Institute (ICSI) for the loss caused due to the cancellation and we shall be liable for penal / legal action including black listing by ICSI.

vi) We understand that ICSI reserves the right to cancel the quotation / tender at any stage or cancel / reject any one or more bid without incurring any liability.

vii) The duly signed copies of all the tender pages are attached herewith.

Date:

Signature _____
(Authorized signatory of the agency)
Name of the bidder_____

THE INSTITUTE OF COMPANY SECRETARIES OF INDIA
ICSI HOUSE, C-36, SECTOR-62, NOIDA -201309

Tender No: PC/IT/Anti-Virus/2019 **13th May, 2019**

Sub: Procurement of Endpoint Protection Anti-Virus Software (Academic Version) Latest Version and Annual Onsite Comprehensive Maintenance Support.

PART 'C' (FINANCIAL BID)

General Specifications/Features of required Endpoint Protection Antivirus Software

1. The Antivirus Software should be an Advanced Endpoint Protection and (latest version) Product.
2. The antivirus software should facilitate the EPO Server and Agent solution including the client end software separately.
3. The Antivirus Software should work on a WAN platform.
4. The antivirus software should have the Enabling / Disabling of On-Demand access scan facility.
5. The antivirus software should be configurable with auto update of virus signatures.
6. The antivirus software should be capable of stopping zero day attacks
7. The antivirus software should be equipped with detection capability of spy ware activities within the system
8. The antivirus system should be equipped with the detection capability to modification of system files and other suspicious activities within the system and throw appropriate alerts to the users
9. The antivirus system should have the capability to perform various types of scanning (e.g. Polymorphic, Heuristic scans etc.)
10. The antivirus software should be configurable to the extent that the end users should not be able to disable the antivirus system on their respective systems.
11. The Antivirus Suite should give a total protection to the systems.

Bill of Quantity for Antivirus Software (Supply, installation & configuration) including All Taxes.

Rates Quoted should be all inclusive rate except GST which should be shown separately as percentage rate (%) (figure in Rs.)

S. No.	Item Description	Qty. (nos.) (a)	HSN/ SAC (b)	Unit Rate per Annum (c)	Total (d=a*c)	GST % (e)	GST amount (f =d*e)	Total per Annum (All Inclusive) (g=d + f)
1	Endpoint Protection Anti-virus Software (latest version) license for 400 nodes including Installations, Configuration with technical principal on-site support services for a period of Three (3) years. (Technical Specs are enclosed in Technical Bid.)	400						
	Grand Total	**400**						
	Total Amount (in Words) ---------- ---------- ----------.							

Note: For the item vendor has to provide the Endpoint Protection Anti-virus Software in CD / DVD / Through Online link with user ID and Password compulsorily along with paper license mentioning the no of license's being procured for the respective software.

DELIVERY: ICSI C-36, Noida Office
Delivery Period Days: _____
Validity of Offer: _____
Any Special Terms (Please Specify):

Date: Name and Signature of Bidder with Corporate Seal