TENDER DOCUMENT

FOR

ANTIVIRUS SOLUTION WITH

EXTRA ANTI RANSOMWARE, MALWARE PROTECTION

&

EMAIL SERVER SECURITY WITH GATEWAY

AT

GUJARAT GREEN REVOLUTION COMPANY LIMITED

Gujarat Green Revolution Company Limited,
Opp. GSFC University, GSFC Fertilizernagar,
Vadodara-391750 (Gujarat)

Phone: 0265-2607515-20, 1800-233-2652,
Fax: 0265-2241685,
Website: www.ggrc.co.in

TENDER DOCUMENTS CONSISTING OF:

E-TENDER NOTICE

1. **GUJARAT GREEN REVOLUTION COMPANY LIMITED (hereafter referred to as GGRC)** is working as an Implementing Agency on behalf of Government of Gujarat (GOG) and Government of India (GOI) to bring second Green Revolution in consonance with the Agriculture Policy and Vision of Government of Gujarat so as to save water, fertilizer and energy, besides multiple benefits to improve agricultural productivity and farmer's prosperity at large.

GGRC is pleased to invite "E-Tenders" through (n) Procure from experienced firm /company /agency for "**TENDER DOCUMENT FOR ANTIVIRUS SOLUTION WITH EXTRA ANTI RANSOMWARE, MALWARE PROTECTION & EMAIL SERVER SECURITY WITH GATEWAY AT GUJARAT GREEN REVOLUTION COMPANY LIMITED"**

2. **Important details of E-Tendering**

Tender No.	:	**GGRC/SYSD/IT SECURITY/RFP/2020-21**
Name of Work	:	**PROVIDING ANTIVIRUS SOLUTION WITH EXTRA ANTI RANSOMWARE, MALWARE PROTECTION & EMAIL SERVER SECURITY WITH GATEWAY AT GUJARAT GREEN REVOLUTION COMPANY LIMITED**
Earnest Money Deposit (in Rs.)	:	Rs. 15000/- (Refundable)
Pre-Bid Meeting Date & Time	:	**12th November,2020 15:00 Hrs**
Pre-Bid Meeting Venue	:	Discussion Room GGRC, Fertilizernagar, Vadodara.
Last Date of Tender and Submission of Document	:	**24th November,2020 17:00 Hrs**

2.1. The financial bid shall be submitted online only at (n) Procure website **www.nprocure.com.** Manual price bids will not be accepted under any circumstances.

Eligibility Criteria:

The eligibility criteria for invitation of bids are mentioned below. Only those Vendors, who satisfy all the eligibility criteria as mentioned herein below, May respond. Document in support of all eligibility criteria are required to be submitted along with technical bid.

1. The vendor should be the original Equipment manufacturer (OEM) or authorized highest efficiency partner of OEM

2. Vendor Must have back support relation with the OEM's whose products are proposed by the vendor to GGRC

3 The vendor should be firm /company registered in India with minimum Five Years of presence in India.

4 The OEM should be in the business of providing antivirus, server security and email security Solution for at least five years as on date of this tender.

5 The OEM Solution offered by the vendor should have been deployed at minimum 4 locations.

6 The Vendor preferable office setup in Vadodara/Ahmedabad, Gujarat.

7 All Licenses/devices that is supplied should be genuine and legal.

8 The Vendor shall not quote for the products, whose end of sale/ End of support has been declared by the OEM and the certificate assuring the same has to be submitted with product having minimum support life 5 years from date of purchase.

9 The Solution proposed, as per Tender RFP specifications, has to be end to end from single OEM.

10 The Bidder should have turnover of minimum Rs. 2.0 Crores per annum for the past 2 financial years

3. The E-Tender are in **two bid system i.e. Part –I- Technical Bid and Part-II -Financial Bid.**

4.1 The Bidders who are interested in participating in the tender must read and comply with the General Terms and Conditions contained in the tender documents.

4.2 Before quoting the rates, the Bidder should go through the Scope of Work, General Terms and Conditions to Bidder, Other Terms & Conditions and get himself fully conversant with them.

4. Company reserves the right to accept or reject any E-Tender Bid without assigning any reasons whatsoever and decision of the Company will be final and binding on all the Bidders.

PART A - GENERAL TERMS AND CONDITIONS

(A) TECHNICAL BID

1. Bidders have to submit **Technical Bid online as per the Format attached at Part -I** Bidder Profile as well as physically in Separate sealed envelope in **Cover-II:** mentioning **"Technical Bid"** with following documents:

1.1. **Bidder has to pay E.M.D. as mentioned in tender notice. The EMD is payable in favour of Gujarat Green Revolution Company Limited, Vadodara Drawn on any Scheduled Commercial Bank / Nationalized Bank by Demand Draft or Banker's Cheque or Direct deposit with Bank of Baroda Account No. 02090200000334, IFSC Code: BARB0FERTIL only.**

Bidder has to upload PDF copy of **DD / Banker's Cheque / Receipt of Direct deposit with (GGRC Bank Account) online as Annexure –I and also has to submit** original **DD / Banker's Cheque / Receipt of Direct deposit with (GGRC Bank Account)**of EMD of Rs. 15,000/- in **Cover –I**: mentioning **"EMD for Tender**. Tenders submitted without Earnest Money Deposit will be rejected without entering in to further correspondence in this regard and no reference will also be made.

The EMD of unsuccessful/successful Bidder will be refunded preferably in 30 days of finalization of the contract. Such deposits shall not bear any interest. It will not be open to the Bidder to withdraw the tender.

If any Bidder withdraws or fails to accept the contract when awarded, the EMD shall be liable to be forfeited.

1.2. Certificate of Registration / Partnership deed or firm registration certificate / Shop and Establishment Certificate. **(Annexure –II)**

1.3. Bank Account No. and IFSC Code with copy of Bank Cheque. **(Annexure- III)**

1.4. EPF Number Allotment Letter (If Applicable) (**Annexure - IV)**

1.5. GST Registration **(Annexure- V)**

1.6. PAN Card**(Annexure-VI)**

1.7. Copy of Work Orders from Previous Clients / Current clients. **(Annexure -VII)**

1.8. Work Performance Certificate from past / Current Client in the **Format attached at (Annexure-VIII)**

1.9. The certified copy of balance sheet for last two years duly audited / certified by Chartered Accountant along with CA certificate for turn over & Net worth and a copy of Un-Audited Balance Sheet for the Current Financial Year to be submitted in physical in Technical bid cover. Last two years Financial Turnover in the Format attached at **Annexure-IX.** GGRC may at its discretion reduce the minimum turn over limit.

1.10. The bidders have to sign undertaking in regard to Stop Deal / Black List Thereof in **(Annexure-X).** This should be submitted with the technical bid.

The Bidder shall submit all the evidences, documents, attested copies of work orders & work completion certificates etc. as a proof with EMD and also provide the requisite details for meeting the prequalification requirements. GGRC will verify the experience, performance, capability & strength of Bidders, independently for awarding the service contract.

GGRC reserves the right to accept/cancel/reject any/all Bids without assigning any reason thereof. The tenders of qualified Bidder / Bidders shall only be considered for further evaluation.

2. The Bidders have to submit original DD / **Banker's Cheque** / Receipt of Direct Bank Deposit (GGRC Bank Account) of **EMD" in Cover –I** and **"Technical Bid"- in Cover –II** with necessary documents mention above in point no.1 in one sealed envelope super scribed **"TENDER DOCUMENT FOR ANTIVIRUS SOLUTION WITH EXTRA ANTI RANSOMWARE, MALWARE PROTECTION & EMAIL SERVER SECURITY WITH GATEWAY AT GUJARAT GREEN REVOLUTION COMPANY LIMITED"** on or before the closing date and time of Tender to the following address:

Sr. Manager System
Gujarat Green Revolution Company Limited,
Fertilizernagar Township, P.O. Fertilizernagar, Dist: Vadodara, 391750

3. Tender documents will be accepted by RPAD / Speed Post / Courier or in Person only otherwise Tender will be rejected.
4. All the certificates/documents required for qualifying criteria should be submitted with Technical Bid for deciding of the opening of financial Bid.
5. GGRC reserves Rights to extend the due date for submission of Tender by issuing an amendment.
5. Tender, if not supported by required documents as mention above will not be considered and the Bidder would be construed as disqualified.
6. The Bidders submitting Tender without EMD or EMD for lesser amount would be construed as disqualified.
7. Any cost incurred in relation with the submission of bid will not be reimbursed by GGRC.
8. **The Bidder must have to submit all required technical documents physically as well as upload online before last date of e-Tender**

(B) FINANCIAL BID

1. The Bidder has to submit **Financial Bid online only as per the attached format given in Part-II** through the web portal of n-procure at **https://www.nprocure.com** of this Tender document and no other format is acceptable.
2. GST if applicable shall be paid extra at actual by GGRC as per prevailing rates as declared by Central / State Government on submission of documentary evidence.
3. The Bidders are requested to note that they should necessarily submit their financial bids in the format provided and no other format is acceptable.
4. The GGRC may on its discretion extend the last date for submission of the bids and such extension shall be binding on all the Bidders. Addendum/Corrigendum/Re-tendering, if any in this regard, will be informed through email.
5. **Financial bid must be submitted online only; if it is found in technical bid physical/online, straightaway bidder will be disqualified.**

(C) MODIFICATION AND WITHDRAWAL OF BIDS:

1. The Bidder may modify or withdraw the bid prior to the last date prescribed for submission of bids.
2. No Bid shall be modified subsequent to the deadline for submission of Bids.
3. No Bid shall be withdrawn in the interval between the deadline for submission of Bids and the expiration of the period of bid validity.

(D) PRE – BID MEETING

1. For the purpose of clarifications of doubts of the Bidders on issues related to the Tender, GGRC intends to hold a Pre-bid meeting. The date and venue of pre-bid meeting is mentioned in the E-Tender Notice.
2. No Individual correspondence will be accepted in this regards.
3. Only authorized representatives of Bidder who can participate and take on the spot decision of the deliberation will be allowed to attend the Pre-bid meeting. A letter to this effect must be carried by the person representing the Bidder at the time of pre bid Meeting.
4. Not more than 3 Representatives would be permitted from each Bidder at the time of the pre bid meeting.

(E) OPENING OF TECHNICAL AND FINANCIAL BID

1. Online Bids (complete in all respect) as well as physically in separate sealed envelope received along with DD / Banker's Cheque / Receipt of Direct Deposit (GGRC Bank Account) of EMD (Physically) on or before closing date and time of tender will be opened. **Bid received without EMD and after due date will be rejected straightaway.**
2. The Technical bid should be complete in all respects, except prices, contain all information asked for and most importantly comply with the technically. The documentary proof in support of all Eligibility Criteria should be submitted along with technical Bid.
3. Incomplete bid or bids not confirming to the terms and conditions are liable for rejection by GGRC. Any Technical Bid, submitted with incorrect information will be liable for rejection. Further, if any Bidder is found to have submitted incorrect information at any time, he may be debarred from participation in the tendering processes.
4. A duly constituted **Tender Evaluation Committee** will evaluate eligibility criteria of bidders. Technical bid of only those bidders, whose bids are declared eligible by the committee, will be evaluated.
5. It shall be noted that required documents submitted in separate sealed envelope along with the Technical bid will be perused/examined and in case of any deficiency, the Technical Bid will be rejected and Financial Bid will not be opened.
6. **Preliminary Examination:**

   6.1 The Company will examine the Bids for any computational errors, for sureties furnished by bidder, for authentication of documents submitted and completeness of the Bids.

   6.2 Arithmetical errors or any discrepancy will be rectified & will be binding to the bidders.

7. **The successful bidder (L-1) shall be decided only after successive tendering procedure by the Tender Evaluation.**

   7.1 GGRC will award the Contract to that bidder whose quotation has been determined to be substantially responsive and evaluated as the lowest quotation in conformity with the requirements of the specifications and documents contained herein, provided further that the bidder is determined and evaluated to be qualified to perform the contract satisfactorily.

   7.2 The successful bidder shall be intimated of his selection through the Letter of Intent or Letter of Award/ Work Order which shall be sent to him through e-mail.

7.3 GGRC reserves the right to seek clarification or call for supporting documents from any of the Bidders, for which the concerned Bidder needs to submit the documentary evidence(s) as required by GGRC.

7.4 GGRC reserves the right to resort to re-tendering without providing any reason whatsoever. GGRC shall not incur any liability on account of such rejection.

7.5 This Tender is non transferable. The incomplete and conditional tenders will be summarily rejected;

7.6 No Bidders will be allowed to withdraw after e-submission of bids/ opening of the tender; otherwise the EMD submitted by the firm will be forfeited;

8 Validity of Bids

8.1 Bids shall remain valid and open for acceptance for a period of 90 days from the last date of submission of Bids.

8.2 The GGRC reserves right to extend for another period of 60 days in addition to 90 days without giving any reasons thereof.

8.3 In case, GGRC calls the bidder for negotiation then this shall not amount to cancellation or withdrawal of original offer which shall be binding on the bidder.

9 Right of Acceptance

9.1 The GGRC reserve all rights to reject any bid including bids of those bidders who fail to comply with the instructions without assigning any reason whatsoever and does not bind it to accept the lowest or any specific bids. The decision of the GGRC in this regard shall be final and binding.

9.2 Any failure on the part of the bidder to observe the prescribed procedure the bidder's bid is liable for rejection.

9.3Any attempt to canvass for the work shall render the bidder's bids liable for rejection.

9.4 The GGRC reserves the right to award any or part or full Contract to any successful Contractor at its sole discretion and this will be binding on the bidders.

9.5 In case of failure to comply with the provisions of the terms and conditions mentioned by the Contractor that has been awarded the Contract, the GGRC reserves the right to award the work to the next higher bidder or any other Contractor and the difference of price shall be recovered from the Contractor, which has been awarded the initial Contract and this will be binding on the bidders. Security Deposit is also forfeited.

9.6 GGRC may terminate the Contract if it is found that the Contractor is blacklisted on previous occasions by any of the Government Departments / Institutions / Local Bodies / Municipalities / Public Sector Undertakings / Private / Limited Companies.

9.7 The Company reserves the right to amend/ modify the Bidding documents at any time prior to the deadline for submission of Bids, either at its own discretion or in response to

the clarification requested by a prospective Bidder. In such case, the Company may in its discretion extend the deadline for submission of Bids in order to facilitate the prospective Bidders for incorporating the effect of the amendment in their Bids.

(F) NOTIFICATION OF AWARD BY ISSUANCE OF 'LETTER OF ACCEPTANCE'

1. After determining the successful bidder after evaluation, the GGRC shall issue a Letter of Acceptance (LOA) in duplicate, which will return one copy to GGRC duly acknowledged, accepted and signed by the authorized signatory, within seven (07) days of receipt of the same by the successful bidders.
2. The issuance of the Letter of Acceptance to the bidder shall constitute an integral part of the Agreement and it will be binding to the Contractor.

(G) PREPARATION OF BIDS

1. Bidder should take into account any corrigendum published on the tender document before submitting their bids.
2. Please note the number of covers in which the bid documents have to be submitted, the number of documents - including the names and content of each of the document that need to be submitted. Any deviations from these may lead to rejection of the bid.
3. Bidder, in advance, should get ready the bid documents to be submitted as indicated in the tender document / schedule.

(H) SUBMISSION OF BIDS

1. The Bidders shall have a valid Class-III digital signature certificate for participation in the online tender. Without Digital Signature online tender process is not possible. The cost of digital signatures, if any, will be borne by respective Bidders. For the same all may contact to following address:

E PROCUREMENT SUPPPORT
(n) Code Solutions
A division of Gujarat Narmada Valley Fertilizers Compnay Ltd.
301, GNFC Info Tower, Bodakdev, Ahmedabad-380054
Ph. 079-26857316/17/18,079-4007501/02/515/525 Fax-079-26857321

2. The Bidders shall have to submit bids before the last date of Tender submission and also as per the terms and conditions mentioned in this document.

(I) ASSISTANCE TO BIDDERS

1. Any queries relating to the tender document and the terms and conditions contained therein should be addressed to **Shri J G Simon, Sr. Manager (Systems) or Shri Jignesh Patel (0265 – 2607518) or in person by visiting the GGRC during working hours (08.30 to 17.00) by taking prior appointment.**

PART B- OTHER TERMS AND CONDITIONS

1. The Rates quoted by bidder shall remain FIRM throughout the Contract period and shall not be subjected to any Price variation whatsoever in nature.

2. The Contractor will deploy manpower for satisfactory execution of the Jobs under the Proposed Contract. The manpower engaged by you will work effectively and be responsible for completion of the Jobs assigned to them by Company's Authorized Person or Contractor.

3. **Security Deposit**

3.1 The successful Bidder have to submit 5% Security Deposit Amount of Total Work order value in favour of "M/s Gujarat Green Revolution Company Limited" payable at Vadodara from any Public Sector Bank or schedule Private Sector Bank to GGRC within 15 days of receiving the Work Order.

3.2 Security Deposit will be released six (6) months after the completion of Work Order period.

3.3 GGRC reserves right to forfeit full Security Deposit amount to cover expenses / damages on non-performance of the contract by the Contractor and / or non-completion of the full period of contract awarded to the Contractor. The decision of GGRC in this regards shall be construed as final and binding.

4. **PENALTY**

Quality of Services will be monitored and in case Quality of Services is not up to the satisfaction of the Head of the Concerned Departments / Unit, following action will be taken:

4.1 For any delay in installation and commissioning of the software Solution beyond the specific period, GGRC will charge penalty @ 0.5% of the order per week or part thereof, subject to a maximum of 5%. In case, the amount equals to 5% of the order value and is deductible as penalty and the vendor is still unable to complete successful Installation, the Institute reserves the right to cancel the order and no payment will be made to the vendor.

4.2 The successful service provider must guarantee fixes to virus infections within maximum 2 hours after being made aware of the virus. Failure to provide fixes within 2 hours will result in an extension on current license period by one week.

5. SUB-LETTING

The contractor shall not sublet the whole or part of the work, except where otherwise provided by the contract. The Contractor shall not sublet any part of the work without the written consent of the concerned Unit OR Department Head and such consent if given shall not relieve the contractor from any liability or obligation under the contract and shall be responsible for the acts, defaults and neglects of any sub-contractor, neglects of the contractor, his agent, servants, or Employee.

6. ASSIGNMENT OR TRANSFER

You will not assign or transfer whole or part of the contract awarded to you hereunder or whole or part of your work, services, obligations, responsibilities, liabilities, and rights, hereunder or give a sub-contract for carrying out all or any of your works, services, obligations, responsibilities, liabilities, and rights hereunder to any other person or party without our prior written consent.

7. PAYMENT TERMS:

Payment shall be released subject to the following:

7.1 No additional payment apart from the tender bid value will be done under any circumstance.

7.2 All the Payments will be made, based on work order with supporting documents evidence etc., Applicable Income Tax will be deducted from the payment.

7.3 Bidder will raise an invoice (hard copy) of completion of work. 100 % Payment will be done within 30 days after receiving an invoice.

8. TERMINATION OF CONTRACT

GGRC reserves the right to cancel the order placed on the selected Bidder by providing one months notice and recover expenditure incurred by GGRC on the following circumstances:

8.1 In case of any changes in GGRC's business plan, GGRC may terminate any part or entire services to be rendered by giving a notice period of one month.

8.2 The selected Bidder commits a breach of any of the terms and conditions of the bid.

8.3 The progress regarding execution of the order accepted, made by the selected Bidder is found to be unsatisfactory.

8.4 If the selected Bidder does not perform satisfactorily or delays execution of the contract, GGRC reserves the right to get the balance contract executed by another party of its choice by giving one month notice for the same. In this event, the selected Bidder is bound to make good the additional expenditure, which GGRC may have to incur in executing the balance of the contract. This clause is applicable, if for any reason, the contract is cancelled.

8.5 In addition to the cancellation of work order, GGRC reserves the right to appropriate the damages through encashment of Performance Guarantee given by the Bidder.

8.6 The bidder shall not assign or sublet his scope of work or any part thereof; any breach of this condition shall entitle the GGRC to terminate contract and selected Bidder liable for payment to the GGRC in respect of any loss or damage arising or ensuing from such termination.

8.7 The Contractor can terminate the Contract by giving three month’s written notice to the Company.

8.8 The Contractor shall prefer a claim for any dues in writing within 30 days from the date of termination or completion of agreement, failing which such claim for any dues shall be deemed to have been waived and the Company shall be discharged and released from all liabilities under this agreement in respect of such claim for any dues.

10. **LANGUAGE OF THE TENDER:**

All information in the bid shall be in English. Information in any other language shall be accompanied by its translation in English. Failure to comply with this may disqualify a bid. In the event of any discrepancy in meaning, the English language copy of all documents shall govern. Notarized copy of certificate / documents provided in Hindi / Gujarati will be accepted.

11. **AMENDMENT OF TENDER**

At any time prior to the deadline for submission of Tender, GGRC, Vadodara for any reason, whether at its own initiative or in response to the clarifications requested by prospective interested bidders, may modify the Tender document by amendment.

The same amendment will be notified in leading newspaper and on GGRC website (www.ggrc.co.in) and changed modification will be binding on them. In order to allow prospective Agencies a reasonable time to take the amendment into account in preparing their Tender document, GGRC, Vadodara, at its discretion, may extend the deadline for the submission of Tender.

12. **REJECTION OF TENDER:**

The Bidder is expected to examine all instructions, terms, conditions, schedules and other details called for in this specification and keep himself fully informed about all which may, in any way, affect the work, or cost thereof. Failure to furnish the required information or submission of tender not as per the specification will be at the Bidder's risk and may result in rejection.

The offer may be rejected in case the bidding schedules / annexure are not filled/ partially filled and if particulars are not given in format prescribed in the tender documents.

13. **INTELLECUAL PROPERTY**

GGRC retains all rights to its pre-existing intellectual property and any intellectual property it creates in connection with the agreement; and the Bidder assigns to organization all rights in any work product developed.

Bidder pursuant to the agreement shall be deemed to be owned by the organization. If the Bidder will not agree to an assignment, then the Bidder should, at a minimum, grant organization a perpetual, irrevocable, worldwide, royalty-free license to use the work product developed pursuant to the agreement.

14. FORCE MAJEURE

14.1 Force majeure is herein defined as any cause, which is beyond the control of the selected Bidder or GGRC as the case may be which they could not foresee or with a reasonable amount of diligence could not have foreseen and which substantially affect the performance, such as:

a. Natural phenomenon, including but not limited to floods, droughts, earthquakes, epidemics, etc.
b. Acts of any Government, including but not limited to war, declared or undeclared, priorities, quarantines, etc
c. Terrorist attacks, public unrest in work area, etc.

14.2 If a Force Majeure situation arises, either party (GGRC & Bidder) shall within ten (10) days from the occurrence of such a cause notify the other in writing of such causes. The Bidder or GGRC shall not be liable for delay in performing his / her obligations resulting from any Force Majeure cause as referred to and / or defined above.

In case of forced circumstances, the contractor may be informed by the Company one Day in advance pertaining to stoppage of full or part of the job work as per the **Scope of Work** explained to you and bill will be paid on the basis of total amount of work performed by the Contractor. For resumption of the work, the contractor will be informed one day in advance.

15. DISCIPLINE

15.1 No information about GGRC can be used by the Bidder in whatsoever circumstances for any purpose. Breach of this will legally be filed as per the Govt. of India IT Act 2008.Permission of GGRC will be required before Bidder uses GGRC's name for any referrals.

15.2 Since the personnel of the Bidder have to work in GGRC, they shall adhere to all administrative and safety requirements of GGRC.

16. SETTLEMENT OF DISPUTES AND ARBITRATION

In case any dispute or difference whatsoever arises between the parties hereto in respect of or relating to or touching this tender and Contract from the tender , then the parties shall try to settle every such dispute or differences amicably. Any such dispute or differences, which the parties cannot resolve in an amicable manner, shall be finally settled in accordance with the Arbitration and Conciliation Act, 1996 and Rules framed there under. The decision of Arbitrator shall be final and binding on the parties. Arbitration proceedings shall be conducted in Vadodara and the language of Arbitration shall be English. Notwithstanding the existence of any such dispute or difference or any reference thereon, the liabilities and obligations under this contract will continue to be fulfilled by the parties hereto during the arbitration proceedings.

17. JURISDICTION OF COURTS:

This shall be construed and governed by the laws of Republic of India and the parties hereby submit to the exclusive jurisdiction of the Vadodara Courts of Law.

18. NON-DISCLOSURE AGREEMENT

Vendor is required to sign a Non-Disclosure Agreement as specified format. This should be submitted after receiving work order.

PART C – Scope of Work & Technical Specification

1. SCOPE OF WORK:-

- Following Security Solution to be provided at GGRC by the Bidder.
  - Antivirus Solution With Extra Anti Ransomware, Malware Protection for Desktop, Laptop, Server (Windows Operating System, Linux)
  - Email Security and gateway with Spam and content filtering
- All Security Solution must be of same make and also with 3 years of warranty.
- Security Solution of OEM acquired companies will not be accepted.
- Supply installation configuration and implementation of total security Solution complying with the technical specifications along with associated software licenses and necessary documents/manuals on site. The costs related to these will be a part of the bid amount and no additional payment will be done by GGRC for the same.
- GGRC reserves the right to change the actual quantity of each of the security Solution to be ordered during the execution of projects. However GGRC will not exceed the tender values as finalized for this bid.
- Security being prime concern, the proposed Solution should not breach the security of any other installation of GGRC in any way.
- Any corruption in the software or media shall be rectified during the full period of the contract at no extra cost to GGRC.
- The Security Solution supplied must be seamlessly integrated with the existing network of GGRC.
- Specialized Antivirus and Anti-RANSOMWARE , malware for servers.
- Initial scanning and cleaning of all PCs/Laptops/Servers etc to be done before installing antivirus Solution with no formatting of devices. Dynamic application containment checking of application for virus.
- Application of machine behavior learning – classification to block zero day threats before they are executed and stop live execution of threats that evaded previous detection.
- By end of every quarter, Bidder has to submit security audit report of all IT peripherals of GGRC where the antivirus solution is installed.
- Remote Support 24X7 for any call reported and Solution to be provided within 1 hour of reporting.
- Escalation matrix for resolving issues with timelines for
  - Remote desktop support issues within 1 hour of reporting.
  - Deployment of personnel within two hours after failure of remote support.
- Faster scanning and uses minimal system resources.
  - Terminating all known virus processes and threads in memory.
  - Repairing the registry.
  - Deleting any drop files created by viruses.
  - Removing any Microsoft Windows services created by Viruses.
- Bidder shall apply all software updates / version upgrades released by the respective OEMs during the contract period.
- In case the bidder has not indicated any peripherals /equipment in their proposed solution and these may be required for the successful implementation of the DLP solution, the successful bidder has to provide the required peripherals/equipment at no additional cost to GGRC.
- Training of all security Items to GGRC IT officials.

Technical Specification

ANTIVIRUS SOLUTION DESKTOP , LAPTOP & SERVER	
Sr. No.	**Description**
1	The Solution should provide multi-layer of protection into a single agent - (AV, NIPS, HIPS, Memory Exploit Mitigation, Advance Machine Learning, Emulation capabilities, Behavioural Monitoring and protection, reputation lookup, application and device control & system lockdown)
2	Network threat protection should analyze incoming data and blocks threats while they travel through the network before hitting the system. Rules-based firewall and browser protection should be included to protect against web-based attacks
3	Signature-based antivirus should eradicate malware on a system to protect against viruses, worms, Trojans, spyware, bots, adware, and root kits and also should offer comprehensive client/server security by protecting enterprise networks from viruses, Trojans, worms, hackers, and network viruses, plus spyware and mixed threat attacks.
4	Correlate different linkages between users, files, and websites to detect rapidly mutating threats. By analyzing key file attributes, The solution should accurately identify whether a file is good and assign a reputation score to each file, effectively protecting against targeted attacks.
5	Have artificial intelligence to provide zero-day protection and stop new and unknown threats by monitoring file behaviours while they execute in real-time to determine file risk. Must be able to reduce the risk of virus/malware entering the network by blocking files with real-time compressed executable files.
6	Remediation and side effect repair engine should aggressively scan infected endpoints to locate Advanced Persistent Threats and remove tenacious malware. Administrator should remotely be able to trigger this and remedy the infection remotely from the management console.
7	The Solution should check for the existence for antivirus software, patches, hot fixes, and other security requirements. For example, the policy may check whether the latest patches have been applied to the operating system.
8	The solution should automatically detects what location a system is connecting from, such as a hotspot, wireless network, or VPN and adjusts the security to offer the best protection for the environment.
9	To address the threats and nuisances posed by Trojans, the solution should be able to do the following: Terminating all known virus processes and threads in memory, repairing the registry, Deleting any drop files created by viruses, removing any Microsoft Windows services created by viruses, restoring all files damaged by viruses, Includes Clean-up for Spyware, Adware etc
10	The solution must be able check whether required software, security patches and hot fixes have not been installed on the endpoint as mandated by organization, the solution should be set to connect to an update server to download and install the required software based on the policy.
11	The solution must have reports that incorporate multi-dimensional analysis and robust graphical reporting in an easy-to-use dashboard.
12	The solution must have group update provider reduces network overhead and decreases the time it takes to get updates by enabling one client to send updates to another, enabling more effective updates in remote locations.
13	Must provide Real-time lock down of client configuration – allow or prevent users from changing settings or unloading/uninstalling the software

14	Users with the scheduled scan privileges can postpone, skip, and stop Scheduled Scan.
15	CPU usage performance control during scanning: 1) Checks the CPU usage level configured on the Web console and the actual CPU consumption on the computer 2) Adjusts the scanning speed if: The CPU usage level is Medium or Low and Actual CPU consumption exceeds a certain threshold
16	Solution should have dashboard to include the latest high risk tasks, search capabilities, recent samples, multiple processing stats, e.g. event count, tasks complete, and risk scores over say last 24 hours
17	The solution should manage single license for windows, Linux and mac Operating Systems and management server should not be separate
18	Must provide a secure Web-based management console to give administrators transparent access to all clients and servers on the network
19	The solution should set up peer-to-peer authentication policy, which can grant or block inbound access to the remote computers that have the client installed.
20	The solution should download content updates from the central server when computers are idle so that it does not affect bandwidth. Must reduce network traffic generated when downloading the latest pattern by downloading only incremental patterns
21	If the endpoint client detects a network attack, solution must automatically activate active response to block all communication to and from the attacking computer
22	Should have role based administration with active directory integration: To create custom role type, To add uses to a predefined role or to a custom role. Shall support grouping of clients into domains for easier administration
23	The solutions should be able expose advanced attacks with precision machine learning, behavioural analytics and threat intelligence minimizing false positives.
24	The Solution should provide report over email, CSV, html or pdf.
25	The solution should be in the leader's quadrant of latest Gartner Report for endpoint security.
26	The solution support plug-in modules designed to add new security features without having to redeploy the entire solution, thereby reducing effort and time needed to deploy new security capabilities to clients and servers across the network
27	The solution should allow definition update to be done manually on management servers. Either by using a machine where internet is available or from there you can copy the files to offline management servers.
28	The solution Should help prevent internal and external security breaches by monitoring application behaviour and controlling file access, registry access, processes that are allowed to run, and devices information can be written to
29	The OEM should be in the leader's quadrant of Gartner Report for endpoint security for the last 3 years.

Add-On Integrated DLP

Sr. No	Description
1	Solution Should Protect sensitive data from unauthorized access and leakage from endpoint with the help of Antivirus Agent only. And also have focused on protecting the users from the external threat of data stealing malware.
2	Solution should have the ability to Immediately protect data by enabling Data Loss Prevention option in the same antivirus Server and Client using the administration console, directory, and user groups
3	Solution should provide real time visibility and control to Monitor, block, and report on the movement of sensitive data, with a real-time view of endpoint status
4	Monitor, block, and report on the movement of sensitive data, with a real-time view of endpoint status

5	Should Monitor, report, or block all network channels such as email clients, FTP, HTTP, and HTTPS, instant messaging, SMB and webmail in terms of Data Loss. Monitor only the transmissions outside the local area network or monitor all transmissions
6	Should also have application channel monitor which will help monitor, report, or block all system and application channels such as data recorders (CD/DVD), peer-to-peer applications, printers, removable storage, synchronization software and even the Microsoft Windows clipboard
7	Should provide option to filter the content with low-impact filtering based on keywords, metadata and regular expressions. Build customized "regex" (regular expressions) to monitor and block specific data
8	Should provide option to customized "regex" (regular expressions) to monitor and block specific data
9	Must be able to send notifications whenever it detects a security risk on any client or during a security risk outbreak, via E-mail, SNMP trap or Event log

Mail Server Security and Gateway

Sr. No	Description
1	Solution must include Virus protection and Spam detection which help to protects computers and data against external threats
2	Solution must offer complete defence against email threats with anti-spam accuracy and anti-virus protection
3	Solution should prevent leaks of confidential data
4	solution should be able to provide multilayer spam protection and threat detection by reviewing senders reputation, Examining the complete context of a message, not just the content, performing deep content analysis, Filtering the URL within a message body, scanning URLs and processing them in real time - as the user opens them - to block malicious sites, providing anti-spam URL reputation check/ URL re-writes, protecting against attack heuristics.
5	Solution should perform deep content analysis that should look for and block malicious web content and that indicate malicious intent.
6	Solution should be able to examine the structure of the content looking for potential risks by using multiple scanning engines that should run in parallel to ensure high performance
7	Solution should be able to examine dynamic content such as scripts by running the scripts within the box or in the OEMs cloud infrastructure and thus monitoring of malicious like hidden redirect or drive-by downloads. If malicious behaviour is detected, the script should not be allowed to pass to the end user and should be blocked.
8	Solution should be able to detect different types of attack scams including but not limited to Phish, Charity, Robbed Abroad, Seminar, Inheritance, Financial URL, Fake Deal, Bank Transfer, Fake Cashier's Check, Money Mule, Loan, Financial Phone etc. This list should be able to change dynamically keeping up with the current trends that attackers use in their attempts to get users to open URLs and/or attachments.
9	Should be support Linux Zimbra mail server
10	Solution should identify image based spam
11	Solution should support the end user digest facility to release the email seamlessly.
12	Solution must have the email defence by testing numerous connection-level data points, including DNS, MX record verification, Sender-Policy Framework (SPF)/ Sender ID Framework (SDIF) verification, and recipient verification
13	Solution should protect organization's reputation when filtering the outbound mail stream for spam in the event an internal system is compromised by malware and becomes a source of spam
14	Solution should Protect against the most advanced forms of spam, phishing, and zombie attacks, as well as addresses the newest forms of blended threats where malware is being delivered through an innocuous URL contained with a spam message
15	Solution must have Advanced anti-phishing techniques to protect end users from scams, fraud, identity theft and malicious code

16	Solution should check for personal safe and blocked lists for valid and invalid senders
17	Solution should provide various options for end user controls including web, email and plug-ins. End user control features should include language selection, individualized spam threshold settings, and safe list/blocked list management
18	Solution should provide LDAP/ Active-Directory integration for Authentication and Sender Verification
19	Solution should include Zero-hour threat detection, message tracing with ability to find phishing messages
20	Solution should have Bi-directional filtering
21	Solution should efficiently scan messages and attachments for potentially malicious code
22	Solution should offer Flexible policies which allow administrators to customize the handling of messages based on the results of virus analysis.
23	Solution should accurately detect and quarantine only those messages associated with an emerging virus, without stopping legitimate email. Instead of quarantining all email with attachment types deemed to be dangerous
24	Solution should be able to identify and prevent a wide variety of inbound and outbound policy violations, including offensive language, harassment, file sharing and many more
25	Solution must Monitor inbound/outbound email message flow, including attachments, for compliance throughout the enterprise.
26	Solution should include Attachment scanning and support for custom or proprietary document types
27	Solution should offer configuration of the Custom policies through a graphical user interface, which allows messages to be analysed and processed, based on a comprehensive list of message attributes
28	Solution must support 125 mailboxes from day one and should be scalable to 500 in future
29	Solution should be able to distinguish between spam and marketing mail from a legitimate source and should also allow users to safely un-subscribe.
30	Solution should allow before an upgrade if box can handle the upgrade and alert admin if utilization exceeds thresholds
31	Solution should allow to generate reports that depict separate entries showing the number of Marketing, Social Media, and Bulk messages caught / identified
32	Solution should also show a sender profile report that shows the number of Marketing, Social, and Bulk messages received from that domain for the designated reporting period
33	Solution should have Web or URL Tracking where it should allow administrators to track the end users who click on URLs that have been rewritten by the Email Security solution OR Solution should have Web or URL reputation check mechanism where it should provide real time lookups for rapidly changing spam content such as URLs, and block the email in real time.
34	Solution should have multiple on-box reports (PDF, Excel, HTML formats) showing the following (but not limited to). • Summary Dashboard • Global Message trends • Attachment Volume/Size trends • Virus Classification trends
35	Solution should support automatic scanning and the use of proven and up-to-date policy filters where emails with sensitive content are encrypted without user action.
36	The Proposed solution should have capabilities to detect Ransomware.
37	Solution should include DLP which offers Dashboard that provides a single, consolidated view of all compliance activity across an organization with real-time statistics, the ability to drill into any specific incident and take immediate action
38	Solution should support secure documents that need to be kept confidential
39	Solution should include Separate processing of unauthorized advertising (the user can choose what to do, to prevent, to subscribe for, reporting)
40	Solution should support encryption feature should work without installing a program

41	The Solution should protect against DoS attacks.
42	Solution should include customized reporting for each customer
43	Solution should include easy managing through a web-based administration portal.
44	Solution should include quarantine management
45	Solution must include Alert monitoring
46	Solution should support the single appliance for centralised reporting, centralised quarantine and compliance incidents
47	Solution should allow administrator to setup Sub-organizations with the Delegated Administration feature
48	Solution should be configurable to work as both Active-Active and Failover Cluster and manageable through a common web based management console.
49	Should include all the required accessories, cables and connectors for mounting in rack and should be supplied with 3-Year OEM Warranty and Support.
Solution Should have the capability to generate User based Alerts and Reports in case of following events	
1	Virus outbreak alert
2	Special virus alert
3	virus found- first and second actions unsuccessful
4	virus found-first action successful
5	virus found-second action successful
6	Network virus alert
7	suspicious vulnerability attack detected
8	**Virus detection reports**
	viruses detected
	Most commonly detected viruses (10,25,50,100)
9	**Antivirus client information reports**
	Detailed/Basic summary
10	**Comparative Reports**
	Spyware/Grayware, Grouped by (Day, Week, Month) RANSOMWARE (Day, Week, Month)
11	**Antivirus server deployment reports**
	Detailed summary
	Basic Summary
	Detailed Failure rate Summary
12	**Network Virus wall reports**
	policy Violation report: policy violations, grouped by (Day, Week, Month)
	Service violation report: Service violations, Grouped by (Day, Week, Month)
	Most common clients in violation: clients with the most violations, (10,25,50,100)

2. CONFIGURATION & ASSOCIATED SERVICES

Following services have to be provided as a part of this tender:

- Configuration of the total security Solution to be installed in laptop, Desktop, Servers and other items, all necessary patches for security Solution must be installed at GGRC.
- Installation and Implementation activities that will be require a downtime of more than 4 hours will be carried out between 6 PM (present day) and 6 AM (following day). This will be done in co-ordination with concerned GGRC Team. A 48-hour notice to be given to GGRC for the same.

3. DELIVERY TERMS

- GGRC reserves the right to place a work/purchase order for entire scope or a part of it.
- The vendor shall supply, install and integrate the security Solution within 4 weeks from date of issue of purchase order.
- Because of teething issues and instant remedial measures a site engineer will be deployed at GGRC for first 1 week after the GO LIVE date for General Shift.
- The project will be deemed to complete when all the products specified in Annexure-XI have been supplied, installed, configured, integrated, and made operational as per the technical specifications and satisfactory acceptance given by GGRC. This will be termed as the "GO LIVE" date.
- The vendor has to resolve any operating system and application software, etc. problems for successful installation and operations.
- Any license, if required need to be provided by the successful Vendor.
- The successful vendor is solely responsible for any legal obligation related to licenses during support period of thirty six (36) months for Solution proposed as implemented by the Vendor.

4. SUPPORT FOR SECURITY SOLUTION

- The Selected Vendor shall provide OEM support for all products that are delivered & installed at sites for a period of 36 Months from the GO LIVE date.
- The product will cover technical on-site support from the vendor and back to back OEM support, software updates, OS upgrades, version upgrades, troubleshooting, TAC support from the OEM, new signature for security Solution and all relevant updates for all to ensure that the most updated security risk library is available at any given point in time.
- During the support period, the vendor will have to undertake preventive maintenance for proper operation, performance and output as specified in the technical specifications of all the security Solution supplied by the vendor.
- During the support period, the vendor should maintain the acceptance criteria and shall be responsible for all costs relating to service, Maintenance (preventive and corrective), technical support and transport charges from and to the sites in connection with the maintenance of the Solution.
- The vendor should inform GGRC about the end of support and end of life of the product proposed.
- The vendor should inform the product life cycle of all the products supplied by the vendor and should specify the product road map in the technical bid.
- The successful Vendor shall endure that services of professionally qualified persons will be available for preventive onsite maintenance of the security Solution during support period. GGRC shall approve the work permission of personal and then only they would be allowed to work on the network. Any other personal will be not allowed to access GGRC network.

Bidders Profile

Performa for Bidders Profile to be uploaded online in PDF format as well as submitted physically with required documents mentioned at "**General Terms and Conditions" specified at Sr. No.1.**

BASIC INFORMATION OF BIDDER

1. Name of the Organization : .....
2. Contact Person : .....
*3. Official Address : .....
.....
.....
.....
4. Mobile No. : .....
5. Telephone No. : .....
6. Fax No. : .....
7. Email Address : _____

8. Details of DD/Banker' Cheque / Direct Deposit in Bank of EMD (As **Annexure-I**) : ……

* Documentary proof of address shall be attested with this Form.

ORGANISATION DETAILS

1. Constitution (whether Sole Proprietorship / Partnership / Private Ltd / Public Ltd. / Public Sector : .....
2. Names of Proprietor/ Partners / Directors / CEO : .....
3. Registration Certificate / Partnership deed / Shop establishment certificate(as **Annexure II**) : .....
4. Bank Details : .....
   Bank Name with branch .....
   Account No. : .....
   IFSC Code : .....
   (Bank Cheque as **Annexure-III**)

REGISTRATION WITH STATUTORY AUTHORITIES

1. EPF Registration (if applicable, as **Annexure-IV**) : .....

2. GST No.: (as **Annexure-V**) : .....

3. PAN No.: (as **Annexure-VI**) : .....

DETAILS OF WORK EXPERINECE & WORK COMPLETION CERTIFICATE

1. Please provide below details of past work experience in reverse chronological order including your current Contracts and attach Work Orders. **(as Annexure VII)**:

SR NO	NAME & ADDRESS OF THE ORGANIZATION	NAME OF THE CONTACT PERSON & PHONE NO.	VALUE OF CONTRACT	PERIOD OF CONTRACT (SPECIFIY FROM TO DATE)
1.				
2.				
3.				

2. Work Performance Certificate from past / Current Client **in the Format attached at Annexure-VIII**
3. Last two years Financial Turnover **in the Format attached at Annexure-IX**

DETAILS OF STAFF AVAILABLE FOR EXECUATTION OF WORK

1. Details of staff available with the company for execution of work (to be submitted online as well as physically with "Technical bid cover." As per Annexure - X)

STATUS OF COMPANY

1. Whether your company was black listed by any company or organization Yes / No (To be submitted online as well as physically as per the Format attached at **Annexure- XI** with "Technical bid cover.") : _____

Signature of Bidder: Name : Designation:		
Date:	Place:	Company's Round Seal

Annexure –I

DD/ **Banker's Cheque of EMD**

Original DD / **Banker's Cheque / Receipt of Direct deposit with Bank** for EMD of Rs. 15,000/- to be submitted online as well as physically in **cover –I.**

Annexure –II

Copy of Registration Certificate / Partnership deed / Shop Establishment Certificate should be **submitted** online as well as physically as **annexure-II** in Technical bid cover- II.

Annexure –III

Copy of Bank Cheque should be submitted online as well as physically as **annexure-III** in Technical bid cover- II

Annexure –IV

Self Attested Copy of EPF no. allotment letter if Applicable should be submitted online as well as physically as **annexure-IV** in Technical bid cover- II

Annexure –V

Self Attested Copy of GST Certificate should be submitted online as well as physically as **annexure-V** in Technical bid cover

Annexure –VI

Self Attested Copy of PAN Card should be submitted online as well as physically as **annexure-VI** in Technical bid cover- II

(Annexure –VII)

Copy of Work Orders from Previous Clients should be submitted online as well as physically as **annexure-VII** in Technical bid cover- II

Annexure –VIII

FORMAT OF WORK PERFORMANCE CERTIFICATE ANNEXURE –VIII

(Filled by Current /Past Clients and to be submitted online as well as physically in Technical bid cover- II**)**

1. Name of the Contract and Location:

2. **Scope of Contract:**

3. **Date of Commencement & Period :**

This is to certify that the work under the above named contract, including all amendments thereto,

has been satisfactorily completed or satisfactorily performing by
……..

Accordance with the terms of the contract.

During the period we found their services satisfactory.

This certificate is issued for tender purpose.

Seal of the Organization

Signature of the Competent Authority with Name and Designation

Date : _____

Place : _____

ANNEXURE –IX

FORMAT FOR FINANCIAL TURNOVER (CAPACITY)
(To be submitted online as well as physically in Technical bid cover- II**)**

CERTIFICATE

This is to certify that M/s._____ having its office at

_____

Has achieved the following turnover during the last Two Financial year.

FINANCIAL YEARS	**ANNUAL TURNOVER (In Rs. CR)**
2018-2019	
2019-2020	

The above figure has been verified from the documents produced and it is true and correct to the best of our knowledge and belief.

Signature of the Chartered Accountant

Name of **Chartered Accountant/ Firm** : .....

Reg. No : .....

.....

Date : _____

Place : _____

Note: It is mandatory to certify by Chartered Accountant (Company Auditor) with name and signature. The certified copy of balance sheet for last two years duly audited / certified by Chartered Accountant along with CA certificate for turn over & Net worth and a copy of Un-Audited Balance Sheet for the Current Financial Year to be submitted in physical in Technical bid cover along with this annexure.

ANNEXURE-X

UNDERTAKING IN REGARD TO STOP DEAL / BLACK LIST THEREOF
(To be filled by bidder and submitted online as well as physically in Technical bid cover- II**)**

Sub: Undertaking in regard to Stop Deal / Black List thereof.
Ref: TENDER NOTICE NO: **GGRC/SYSD/IT SECURITY/RFP/2020-21**

I / We _____authorized signatory of M/S _____hereby declare that M/S _____ is not stop deal/blacklisted by GGRC/ GSFC or its subsidiary companies or by any Central/State Government PSU / Govt. Company or by any Central/State Government Department in India.

Note: Bidders has to reproduce above declaration in the text box area with filling of all blanks

Above furnished is true and correct to best of my knowledge.

Signature of Bidder: Name : Designation	
Place:	Company's Round Seal:

IT security Solution

Annexure- XI

Sr. No	Type of Device	Quantity
1	Antivirus solution with Extra anti RANSOMWARE, malware protection DESKTOP , LAPTOP & SERVER	200
2	Email Security with gateway with Spam and content filtering	125

Bidders Eligibility Criteria Annexure- XII

Sr. No	Criteria	Compliance (YES/NO)	Proof to be submitted
1	The vendor should be the original Equipment manufacturer (OEM) or authorized highest efficiency partner of OEM		Documentary proof to be submitted of OEM or Documentary proof of authorized Highest efficiency partner letter issued by OEM authorizing partner for valid period of Quotation
2	Vendor Must have back support relation with the OEM's whose products are proposed by the vendor to GGRC		Manufacturer's authorization Form/Letter must be submitted along with the bid.
3	The vendor should be firm /company registered in India with minimum Five Years of presence in India		Certificate of Incorporation to be provided. Proof of orders of similar nature over a period of last five years
4	The OEM should be in the business of providing antivirus, server security and email security Solution for at least five years as on date of this tender		Certification/Undertaking letter from OEM is to be submitted clearly mentioning the details and projects where Solution is implemented and providing support
5	The OEM Solution offered by the vendor should have been deployed at minimum 4 locations		Documentary proof should be provided in support of installation base like order copy/contract copy/certificate from customer
6	The Vendor preferable office setup in Vadodara/ahmedabad, Gujarat.		List of support Centres in Baroda/Ahmedabad to be provided
7	All Licenses/devices that is supplied should be genuine and legal		Vendor shall provide in writing an indemnity that all the licenses/devices proposed in this bid is legal
8	The Vendor shall not quote for the products, whose end of sale/ End of support has been declared by the OEM and the certificate assuring the same has to be submitted with product having minimum support life 5 years from date of purchase		Vendor to provide the following documents: 1) Certificate from the OEM assuring that the proposed Solution has not reach end-of-life and end-of-support. 2) Authorization letter of the OEM stating the product has the most recent/stable version of the operating system that is to be installed at the site. 3) Authorization letter of the manufacturer stating the product has the most recent/stable hardware device that is to be installed at the site for all the Solution.
9	The Solution proposed , as per Tender RFP specifications, has to be end to end from single OEM		Documentary proof to be submitted.
10	The Bidder should have turnover of minimum Rs. 2.0 Crores per annum for the past 2 financial years		last two years duly audited / certified by Chartered Accountant along with CA certificate

Part I Technical Bid

ANTIVIRUS SOLUTION DESKTOP , LAPTOP & SERVER			
Sr. No	**Description**	**Compliance (Y/N)**	**Remark**
1	The Solution should provide multi-layer of protection into a single agent - (AV, NIPS, HIPS, Memory Exploit Mitigation, Advance Machine Learning, Emulation capabilities, Behavioural Monitoring and protection, reputation lookup, application and device control & system lockdown)		
2	Network threat protection should analyze incoming data and blocks threats while they travel through the network before hitting the system. Rules-based firewall and browser protection should be included to protect against web-based attacks		
3	Signature-based antivirus should eradicate malware on a system to protect against viruses, worms, Trojans, spyware, bots, adware, and root kits and also should offer comprehensive client/server security by protecting enterprise networks from viruses, Trojans, worms, hackers, and network viruses, plus spyware and mixed threat attacks.		
4	Correlate different linkages between users, files, and websites to detect rapidly mutating threats. By analyzing key file attributes, The solution should accurately identify whether a file is good and assign a reputation score to each file, effectively protecting against targeted attacks.		
5	Have artificial intelligence to provide zero-day protection and stop new and unknown threats by monitoring file behaviours while they execute in real-time to determine file risk. Must be able to reduce the risk of virus/malware entering the network by blocking files with real-time compressed executable files.		
6	Remediation and side effect repair engine should aggressively scan infected endpoints to locate Advanced Persistent Threats and remove tenacious malware. Administrator should remotely be able to trigger this and remedy the infection remotely from the management console.		
7	The Solution should check for the existence for antivirus software, patches, hot fixes, and other security requirements. For example, the policy may check whether the latest patches have been applied to the operating system.		
8	The solution should automatically detects what location a system is connecting from, such as a hotspot, wireless network, or VPN and adjusts the security to offer the best protection for the environment.		

9	To address the threats and nuisances posed by Trojans, the solution should be able to do the following: Terminating all known virus processes and threads in memory, repairing the registry, Deleting any drop files created by viruses, removing any Microsoft Windows services created by viruses, restoring all files damaged by viruses, Includes Clean-up for Spyware, Adware etc		
10	The solution must be able check whether required software, security patches and hot fixes have not been installed on the endpoint as mandated by organization, the solution should be set to connect to an update server to download and install the required software based on the policy.		
11	The solution must have reports that incorporate multi-dimensional analysis and robust graphical reporting in an easy-to-use dashboard.		
12	The solution must have group update provider reduces network overhead and decreases the time it takes to get updates by enabling one client to send updates to another, enabling more effective updates in remote locations.		
13	Must provide Real-time lock down of client configuration – allow or prevent users from changing settings or unloading/uninstalling the software		
14	Users with the scheduled scan privileges can postpone, skip, and stop Scheduled Scan.		
15	CPU usage performance control during scanning: 1) Checks the CPU usage level configured on the Web console and the actual CPU consumption on the computer 2) Adjusts the scanning speed if: The CPU usage level is Medium or Low and Actual CPU consumption exceeds a certain threshold		
16	Solution should have dashboard to include the latest high risk tasks, search capabilities, recent samples, multiple processing stats, e.g. event count, tasks complete, and risk scores over say last 24 hours		
17	The solution should manage single license for windows, Linux and Mac Operating Systems and management server should not be separate		
18	Must provide a secure Web-based management console to give administrators transparent access to all clients and servers on the network		
19	The solution should set up peer-to-peer authentication policy, which can grant or block inbound access to the remote computers that have the client installed.		
20	The solution should download content updates from the central server when computers are idle so that it does not affect bandwidth. Must reduce network traffic generated when downloading the latest pattern by downloading only incremental patterns		

21	If the endpoint client detects a network attack, solution must automatically activate active response to block all communication to and from the attacking computer		
22	Should have role based administration with active directory integration: To create custom role type, To add uses to a predefined role or to a custom role. Shall support grouping of clients into domains for easier administration		
23	The solutions should be able expose advanced attacks with precision machine learning, behavioural analytics and threat intelligence minimizing false positives.		
24	The Solution should provide report over email, CSV, html or pdf.		
25	The solution should be in the leader's quadrant of latest Gartner Report for endpoint security.		
26	The solution support plug-in modules designed to add new security features without having to redeploy the entire solution, thereby reducing effort and time needed to deploy new security capabilities to clients and servers across the network		
27	The solution should allow definition update to be done manually on management servers. Either by using a machine where internet is available or from there you can copy the files to offline management servers.		
28	The solution Should help prevent internal and external security breaches by monitoring application behaviour and controlling file access, registry access, processes that are allowed to run, and devices information can be written to		
29	The OEM should be in the leader's quadrant of Gartner Report for endpoint security for the last 3 years.		
Add-On Integrated DLP			
Sr. No	**Description**	**Compliance (Y/N)**	**Remark**
1	Solution Should Protect sensitive data from unauthorized access and leakage from endpoint with the help of Antivirus Agent only. And also have focused on protecting the users from the external threat of data stealing malware.		
2	Solution should have the ability to Immediately protect data by enabling Data Loss Prevention option in the same antivirus Server and Client using the administration console, directory, and user groups		
3	Solution should provide real time visibility and control to Monitor, block, and report on the movement of sensitive data, with a real-time view of endpoint status		
4	Monitor, block, and report on the movement of sensitive data, with a real-time view of endpoint status		

5	Should Monitor, report, or block all network channels such as email clients, FTP, HTTP, and HTTPS, instant messaging, SMB and webmail in terms of Data Loss. Monitor only the transmissions outside the local area network or monitor all transmissions		
6	Should also have application channel monitor which will help monitor, report, or block all system and application channels such as data recorders (CD/DVD), peer-to-peer applications, printers, removable storage, synchronization software and even the Microsoft Windows clipboard		
7	Should provide option to filter the content with low-impact filtering based on keywords, metadata and regular expressions. Build customized "regex" (regular expressions) to monitor and block specific data		
8	Should provide option to customized "regex" (regular expressions) to monitor and block specific data		
9	Must be able to send notifications whenever it detects a security risk on any client or during a security risk outbreak, via E-mail, SNMP trap or Event log		

Mail Server Security with Gateway

Sr. No	Description	Compliance (Y/N)	Remark
1	Solution must include Virus protection and Spam detection which help to protects computers and data against external threats		
2	Solution must offer complete defence against email threats with anti-spam accuracy and anti-virus protection		
3	Solution should prevent leaks of confidential data		
4	solution should be able to provide multilayer spam protection and threat detection by reviewing senders reputation, Examining the complete context of a message, not just the content, performing deep content analysis, Filtering the URL within a message body, scanning URLs and processing them in real time - as the user opens them - to block malicious sites, providing anti-spam URL reputation check/ URL re-writes, protecting against attack heuristics.		
5	Solution should perform deep content analysis that should look for and block malicious web content and that indicate malicious intent.		
6	Solution should be able to examine the structure of the content looking for potential risks by using multiple scanning engines that should run in parallel to ensure high performance		

7	Solution should be able to examine dynamic content such as scripts by running the scripts within the box or in the OEMs cloud infrastructure and thus monitoring of malicious like hidden redirect or drive-by downloads. If malicious behaviour is detected, the script should not be allowed to pass to the end user and should be blocked.		
8	Solution should be able to detect different types of attack scams including but not limited to Phish, Charity, Robbed Abroad, Seminar, Inheritance, Financial URL, Fake Deal, Bank Transfer, Fake Cashier's Check, Money Mule, Loan, Financial Phone etc. This list should be able to change dynamically keeping up with the current trends that attackers use in their attempts to get users to open URLs and/or attachments.		
9	Should be support Linux Zimbra mail server		
10	Solution should identify image based spam		
11	Solution should support the end user digest facility to release the email seamlessly.		
12	Solution must have the email defence by testing numerous connection-level data points, including DNS, MX record verification, Sender-Policy Framework (SPF)/ Sender ID Framework (SDIF) verification, and recipient verification		
13	Solution should protect organization's reputation when filtering the outbound mail stream for spam in the event an internal system is compromised by malware and becomes a source of spam		
14	Solution should Protect against the most advanced forms of spam, phishing, and zombie attacks, as well as addresses the newest forms of blended threats where malware is being delivered through an innocuous URL contained with a spam message		
15	Solution must have Advanced anti-phishing techniques to protect end users from scams, fraud, identity theft and malicious code		
16	Solution should check for personal safe and blocked lists for valid and invalid senders		
17	Solution should provide various options for end user controls including web, email and plug-ins. End user control features should include language selection, individualized spam threshold settings, and safe list/blocked list management		
18	Solution should provide LDAP/ Active-Directory integration for Authentication and Sender Verification		
19	Solution should include Zero-hour threat detection, message tracing with ability to find phishing messages		
20	Solution should have Bi-directional filtering		
21	Solution should efficiently scan messages and attachments for potentially malicious code		

22	Solution should offer Flexible policies which allow administrators to customize the handling of messages based on the results of virus analysis.		
23	Solution should accurately detect and quarantine only those messages associated with an emerging virus, without stopping legitimate email. Instead of quarantining all email with attachment types deemed to be dangerous		
24	Solution should be able to identify and prevent a wide variety of inbound and outbound policy violations, including offensive language, harassment, file sharing and many more		
25	Solution must Monitor inbound/outbound email message flow, including attachments, for compliance throughout the enterprise.		
26	Solution should include Attachment scanning and support for custom or proprietary document types		
27	Solution should offer configuration of the Custom policies through a graphical user interface, which allows messages to be analysed and processed, based on a comprehensive list of message attributes		
28	Solution must support 125 mailboxes from day one and should be scalable to 500 in future		
29	Solution should be able to distinguish between spam and marketing mail from a legitimate source and should also allow users to safely un-subscribe.		
30	Solution should allow before an upgrade if box can handle the upgrade and alert admin if utilization exceeds thresholds		
31	Solution should allow to generate reports that depict separate entries showing the number of Marketing, Social Media, and Bulk messages caught / identified		
32	Solution should also show a sender profile report that shows the number of Marketing, Social, and Bulk messages received from that domain for the designated reporting period		
33	Solution should have Web or URL Tracking where it should allow administrators to track the end users who click on URLs that have been rewritten by the Email Security solution OR Solution should have Web or URL reputation check mechanism where it should provide real time lookups for rapidly changing spam content such as URLs, and block the email in real time.		
34	Solution should have multiple on-box reports (PDF, Excel, HTML formats) showing the following (but not limited to). • Summary Dashboard • Global Message trends • Attachment Volume/Size trends • Virus Classification trends		
35	Solution should support automatic scanning and the use of proven and up-to-date policy filters where emails with sensitive content are encrypted without user action.		

36	The Proposed solution should have capabilities to detect Ransomware.		
37	Solution should include DLP which offers Dashboard that provides a single, consolidated view of all compliance activity across an organization with real-time statistics, the ability to drill into any specific incident and take immediate action.		
38	Solution should support secure documents that need to be kept confidential		
39	Solution should include Separate processing of unauthorized advertising (the user can choose what to do, to prevent, to subscribe for, reporting)		
40	Solution should support encryption feature should work without installing a program		
41	The Solution should protect against DoS attacks.		
42	Solution should include customized reporting for each customer		
43	Solution should include easy managing through a web-based administration portal.		
44	Solution should include quarantine management		
45	Solution must include Alert monitoring		
46	Solution should support the single appliance for centralised reporting, centralised quarantine and compliance incidents		
47	Solution should allow administrator to setup Sub-organizations with the Delegated Administration feature		
48	Solution should be configurable to work as both Active-Active and Failover Cluster and manageable through a common web based management console.		
49	Should include all the required accessories, cables and connectors for mounting in rack and should be supplied with 3-Year OEM Warranty and Support.		

Solution Should have the capability to generate User based Alerts and Reports in case of following events			
Sr. No	**Description**	**Compliance (Y/N)**	**Remark**
1	Virus outbreak alert		
2	Special virus alert		
3	virus found- first and second actions unsuccessful		
4	virus found-first action successful		
5	virus found-second action successful		
6	Network virus alert		
7	suspicious vulnerability attack detected		
8	**Virus detection reports** • viruses detected • Most commonly detected viruses (10,25,50,100)		
9	**Antivirus client information reports**		

	• Detailed/Basic summary		
10	**Comparative Reports** • Spyware/Grayware, Grouped by (Day, Week, Month) • RANSOMWARE (Day, Week, Month)		
11	**Antivirus server deployment reports** • Detailed summary • Basic Summary • Detailed Failure rate Summary		
12	**Network Virus wall reports** • policy Violation report: policy violations, grouped by (Day, Week, Month) • Service violation report: Service violations, Grouped by (Day, Week, Month) • Most common clients in violation: clients with the most violations, (10,25,50,100)		

PART II Financial Bid

(To be submitted online only)

Financial Bid of Antivirus and Email Security with gateway Solution (Amount in ₹)

Sr No	Item Description	Period (Year)	License Quantity (A)	Unit Price Excluding Tax in Rs. (B)	Total Amount Excluding Tax in Rs. C=A*B
1	Antivirus solution with Extra anti RANSOMWARE, malware protection Desktop, Laptop, and server.	3 Year	200		
2	Email Security and gateway with Spam and content filtering	3 Year	125		
3	Antivirus solution with Extra anti RANSOMWARE, malware protection Desktop, Laptop, and server.	2 Year	200		
4	Email Security and gateway with Spam and content filtering	2 Year	125		

Note: Tax percentage extra as applicable.

CHECKLIST

(TO BE SUBMITTED ONLINE AS WELL AS PHYSICALLY FORM IN SEAL COVER OF "EMD COVER DOCUMENTS" AS WELL AS "TECHNICAL BID COVER DOCUMENTS")

SR NO	NAME OF DOCUMENT	SUBMITTED YES / NO
1.	**Bidders Profile**	
2.	Original DD / **Banker's Cheque / Receipt of Direct deposit with Bank (GGRC Bank Account)** of EMD of Rs. 15,000/- Physically in **cover –I**	
3.	Registration Certificate / Partnership deed / Shop Establishment Certificate. **(Annexure –II)**	
4.	Copy of Bank Cheque **(Annexure –III)**	
5.	Self Attested Copy of EPF no. allotment letter if Applicable **(Annexure –IV)**	
6.	Self Attested Copy of GST Certificate **(Annexure –V)**	
7.	Self Attested Copy of PAN Card **(Annexure –VI)**	
8.	Copy of Work Orders from Previous Clients / Current clients **(Annexure –VII)**	
9.	Format of work Performance Certificate (to be filled by past / Current Client)**(Annexure –VIII)**	
10.	**Format for financial turnover (capacity) Annexure –IX and** Attested Copy of the Audited Balance Sheets for the completed two Financial Years and unaudited balance sheets of current year physically along with Annexure –IX.	
11.	Undertaking in regard to Stop Deal / Black List**(Annexure-X)**	
12	IT Solution **(Annexure-XI)**	
13	Eligibility Criteria **(Annexure-XII)**	
14	PART -I- Technical Bid	
15	PART-II-Financial Bid **(To be submitted online only)**	

Signature of Bidder: Name : Designation	
Place:	Company's Round Seal: