

Response to Pre – Bid Queries

1. C-Edge Technologies Ltd.					
Sr No.	RFP No. & Page No.	RFP Clause	Suggestion/Deviation/Remark	Bank's Remarks	Clauses in the Revised tender Document After Pre Bid
1	NA	General	Request bank to provide atleast 10 days extension for submitting the final bid documents after sharing the response to the queries raised from bidder end.	The date for submission of bid is extended upto 04.01.2022	
2	Page No. 3 Clause No. 6.(8) Bidders Eligibility Criteria	The Bidder shall provide references (including Referee names and contact details) in respect of major projects of similar type completed in the last three(3) years by the Bidder in any large organization and having its offices/branches across India.	Request bank to provide clarity on the references to be shared with bank. References in regards to the completion of major projects to be given of 3 years or 5 years. Request bank to provide clarity on the number of client references to be provided and also request bank to provide clarity on satisfactory letter and purchase order both to be submitted at the time of final bid submission or either one reference can suffice the requirement.	Any proof of having supplied and installed the proposed solution is acceptable.	Page No. 3 Clause No.6 (8)
3	Page No. 5 Clause No. 9 (1) Scope of Work	The “Total solution” will include Supply and Installation of Enterprise Anti-Virus Software License on the infrastructure mentioned below: a) Windows XP SP3 32-bit Edition b) Windows XPSP3 64-bit Edition c) Windows 7 d) Windows 8 e) Windows8.1 f) Windows10 and all future Windows desktop Operating System, 32-bit version & 64-bit version1.	Request bank to define the count for each of the infrastructure/devices mentioned in the clause wherein anti-virus software to be installed. Request bank to provide clarity on the set-up part to be created by the bidder. Can one customized set-up be provided for all the infrastructure/devices mentioned in the clause or bidder to provide dedicated set-up for each type of infratructure/device mentioned in the clause.Request bank to define the count for each of the infrastructure/devices mentioned in the clause wherein anti-virus software to be installed. Request bank to provide clarity on the set-up part to be created by the bidder. Can one customized	Request not considered.	Page No. 5 Clause No. 12 (1)

			set-up be provided for all the infrastructure/devices mentioned in the clause or bidder to provide dedicated set-up for each type of infrastructure/device mentioned in the clause.		
4	Page No. 6 Clause No. 9 (5) Scope of Work	The bidder should fix all the technical problems, provide and implement upgrades, updates free of cost to the Bank, as and when released by the OEM during license period.	Request bank to consider, "The bidder should fix all the technical problems, provide and implement upgrades, updates on mutually agreed commercials with the Bank, as and when released by the OEM during license period".	No change in the clause of bid document.	Page No. 6 Clause No. 12(5)
5	Page No. 6 Clause No. 9 (6) Scope of Work	6. The bidder shall address statutory requirements, network and security audit recommendations suggested by the Bank from time to time on regular basis without additional cost to the Bank.	Request bank to consider below modification; The bidder shall address statutory requirements, network and security audit recommendations suggested by the Bank from time to time on regular basis on mutually agreed cost with the Bank. Request bank to consider below modification; The bidder shall address statutory requirements, network and security audit recommendations suggested by the Bank from time to time on regular basis on mutually agreed cost with the Bank.	No change in the clause of bid document.	Page No. 6 Clause No. 12 (6)
6	Page No. 6 Clause No. 9 (9) Scope of Work	Software maintenance, and Support: a) The bidder shall provide free maintenance services during the period of years. During license period, the bidder shall provide upgrades, updates, patches and regular virus signature updates, etc. Without any additional cost. During the contract period, the bidder must depute qualified maintenance engineer whenever required.	Request bank to consider below modifications; a) The bidder shall provide free maintenance services during the period of years. During license period, the bidder shall provide upgrades, updates, patches and regular virus signature updates, etc. on mutually agreed cost. During the contract period, the bidder must depute qualified maintenance engineer whenever required.	No change in the clause of bid document.	Page No. 6 Clause No. 12 (9)
7	Page No. 6 Clause No. 9 (8) Scope of Work	The Bank shall promptly notify the bidder in writing of any claims arising under this license. Upon receipt of such notice, the bidder shall with all reasonable speed,	Request bank to consider below modification; The Bank shall promptly notify the bidder in writing of any claims arising under this license. Upon receipt of such notice, the bidder shall with all	No change in the clause of bid document.	Page No. 6 Clause No. 12 (8)

		repair or replace the defective products or part thereof without cost to the Bank.	reasonable speed, repair or replace the defective products or part thereof on mutually agreed cost with the Bank based on the efforts involved.		
8	Page No. 6 Clause No. 10 Training	Training A Comprehensive training shall be the key to successful Operations and Maintenance; hence, the Bidder is required to provide required training to the Bank nominated Officials at The Kangra Central Co Operative Bank Ltd, Dharamshala	Request bank to provide below information; 1. Number of bank officials to be trained 2. Number of days and in how many shifts training to be undertaken. 3. Training location 4. Training infra to be provided by bank or bidder to arrange the same.	No change in the clause of bid document.	Page No. 6 Clause No. 13
9	Page No. 8 Clause No. 15 Delivery & Installation Period	a) Delivery \leq 4 Weeks b) Installation and Operationalization \leq 4 Weeks	Request bank to provide 4 months timeline for end to end delivery, installation and operationalization of the solution. We also request bank to consider end to end installation and implementation of 1200 device in 216 branches of bank remotely as bank is located on hilly areas it would be a major challenge for engineers to reach each bank branch location and install and implement the anti-virus solution. We request bank to consider remote installation and implementation of all the devices of 216 bank branches.	Total project should be completed within 8 weeks.	Page No. 7 Clause No. 19
10	Page No. 8 Clause No. 17(b) Obligations of Successful Bidder	The successful bidder shall deploy their own trained and experienced engineers for implementing, managing and maintaining the system.	Request bank to provide below information; 1. Number of resources required for post Go-live Support 2. Number of shifts 3. Support to be provided onsite/offsite/remotely	No change in the clause of bid document..	Page No. 8 Clause No. 21
11	NA	General	We request bank to consider remote implementation, looking at the current covid situation.	Request not considered	
12	NA	General	We request bank to provide clarity on the current bandwidth on which devices are connected for implementation of the proposed solution	It is sufficient for implementaion of anti virus solution. However, the bidder may provide requirement of bandwidth for their solution.	

13	Page No. 6 Clause No. 9 (9) (b) Scope of Work	The bidder shall ensure that faults and failures intimated by the Bank as above are set right within 24 hours of being informed of the same.	We request bank to consider, "b) The bidder shall ensure that faults and failures intimated by the Bank as above are set right within 72 hours of being informed of the same".	The bidder shall ensure that faults and failures intimated by the Bank as above are set right within 48 hours of being informed of the same	Page No. 6 Clause No. 12 (9) (b)
14	Page No. 7 Clause No. 13 Confidentiality	Bidder agrees that all mails, data, financial, mail architecture and personnel data relating to Bank's business and other information identified as confidential by the Bank, the same shall be kept confidential and shall not be shared with any third party without prior written approval from Bank.	Bidder suggest below additions: Company shall not be liable for disclosure or use of any materials or information provided by BANK or developed by Company which is: i) Possessed by Company prior to receipt from BANK, other than through prior disclosure by BANK, as documented by Company's written records; ii) Published or available to the general public otherwise than through a breach of Confidentiality; iii) Obtained by Company from a third party with a valid right to make such disclosure, provide that said third party is not under a confidentiality obligation to BANK; iv) Developed independently by the Company. v) Disclosed by the Bank to another without any confidentiality obligations. In the event that Company is required by judicial or administrative process to disclose any information or materials required to be held confidential hereunder, Company shall promptly notify BANK and allow BANK a reasonable time to oppose such process before making disclosure. Nothing contained in this contract shall limit the Company from providing similar services to any third parties or reusing the skills, know-how, and experience gained by the employees in providing the services contemplated under this contract. The receiving	No change in the clause of bid document..	Page No. 7 Clause No. 17

			party undertakes to (i) hold all such Confidential Information in strictest confidence, (ii) not to disclose such Confidential Information either in whole or in part to any person other than those of its officers, employees and agents who need to know such Confidential Information for the purpose authorized hereunder provided that each such officer, employee or agent has agreed in writing to maintain the confidentiality of such Confidential Information in accordance with the terms hereof and (iii) not to use such Confidential Information for any purpose whatsoever save as may be strictly necessary in connection with the Services provided under this Agreement.		
15	Page No. 8 Clause No. 14 Right to Verification	The Bank reserves the right to verify any or all statements made by the Bidder in the tender document and to inspect the Bidder's facility, if necessary, to establish to its satisfaction about the Bidder's capacity to perform the job.	Bidder suggests below modifications: The Bank reserves the right to verify any or all statements made by the Bidder in the tender document if necessary, to establish to its satisfaction about the Bidder's capacity to perform the job.	No change in the clause of bid document..	Page No. 7 Clause No. 18
16	Page No. 8 Clause No. 17 (d) Obligations of Successful Bidder	The bidder/successful bidder to ensure that during implementation of complete, the critical services hosted at the Bank shall not face any downtime due to security breach, security incident, improper configuration of security units/ appliances/ components.	Bidder suggests below modifications: d. The bidder/successful bidder to ensure that during implementation of complete, the critical services hosted at the Bank shall not face any downtime due to improper configuration of application/components	No change in the clause of bid document..	Page No. 8 Clause No. 21 (d)
17	Page No. 8 Clause No. 18 Order Cancellation:	Bank reserves its right to cancel the order in the event of delay in delivery and installation beyond the stipulated time	Bidder suggests below modifications: Bank reserves its right to cancel the order in the event of delay in delivery and installation beyond the stipulated time and mutually extended time.	No change in the clause of bid document.	Page No. 8 Clause No. 22
18	Page No. 9 Clause No. 19 Penalty	For any delay in installation and commissioning of the	Request bank to consider penalties applicable to those bank branch locations where	No change in the clause of bid document..	Page No. 8 Clause No. 23

	for Delay:	software solution beyond the specific period, Bank 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 bidder is still unable to complete successful Installation, the Bank reserves the right to cancel the order and no payment will be made to the bidder.	bidder can easily install software and bank branches are easily accessible remotely with high network connectivity. Request bank to waveoff penalties for REMOTE Areas/locations of bank branches where there is low network connectivity and for those branches penalty can be mutually decided at the time of actual installation.		
19	Page No. 9 Clause No. 20 Penalty for Undetected Virus/Infection/Malware	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.	Request bank to consider below modifications; The successful service provider must guarantee fixes to virus infections within maximum 2 working days online support after being made aware of the virus. Failure to provide fixes within 2 working days online support will result in an extension on current license period by one week.	The successful service provider must guarantee fixes to virus infections within maximum 24 hrs after being made aware of the virus. Failure to provide fixes within 24 hrs online support will result in an extension on current license period by one week.	Page No. 8 Clause No 24
20	Page No. 9 Clause No. 21 Resolution of Disputes	Bank and the bidder shall make every effort to resolve amicably, by direct informal negotiation, any disagreement or dispute arising between them under or in connection with the contract. If after thirty days from the commencement of such informal negotiations, Bank and the bidder have been unable to resolve amicably a contract dispute, either party may require that the dispute be referred for resolution by formal arbitration.	Bidder suggests below additions: Bank and the bidder shall make every effort to resolve amicably, by direct informal negotiation, any disagreement or dispute arising between them under or in connection with the contract. If after thirty days from the commencement of such informal negotiations, Bank and the bidder have been unable to resolve amicably a contract dispute, either party may require that the dispute be referred for resolution by formal arbitration. The said dispute shall be subject to resolution by arbitration in accordance with the Arbitration & Conciliation Act, 1996. The dispute shall be referred to a mutually agreed sole arbitrator and	No change in the clause of bid document..	Page No. 8 Clause no. 25

			<p>failing such agreement the dispute shall be referred to a tribunal comprising of three arbitrators, one arbitrator shall be appointed by each party and the third arbitrator shall be mutually appointed by the arbitrators so appointed. The language of the arbitration shall be English and the decision of the arbitrator/majority arbitrators as the case may be, shall be final and binding on the parties. The venue of Arbitration shall be Mumbai.</p>		
21	<p>Page No. 9 Clause No. 22 (4) Indemnification</p>	<p>4. The bidder shall also be liable to indemnify the Bank, at its own cost and expenses, against all losses/damages, which the Bank may suffer on account of violation by the bidder/successful bidder of any or all national/international trade laws, norms, standards, procedures, etc.</p>	<p>Bidder shall have no obligations with respect to any claims to the extent that the claim arises or results from: (i) Bidder's compliance with the BANK's specific technical designs or instructions; or (ii) Inclusion in the Deliverables and/or Services of any content or other materials provided by BANK and if the claim relates to or arises from any Customer provided material; or (iii) Modification, alteration, adjustment of the Deliverables and/or Services after delivery by the Bidder to the BANK, if such modification, alteration, adjustment was not made by or on behalf of Bidder; or (iv) Operation or use of some or all of the Deliverables and/or Services in combination with products, information, specification, instructions, data, materials not provided by Bidder; or (v) use of the Deliverables and/or Services for any purposes for which the same have not been designed or developed or other than in accordance with any applicable specifications or documentation provided under the agreement; or (vi) Use of a superseded or altered release of some or all of the Deliverables or any modification thereof furnished</p>	<p>No change in the clause of bid document..</p>	<p>Page No. 9 Clause No. 26 (4)</p>

			<p>under this Agreement including, but not limited to the BANK's failure to use corrections, fixes, or enhancements made available by Bidder. BANK covenants that all software, information, data or material provided to the Bidder in connection with the provision of Services are either owned by it or under license from third parties, with right and liberty to BANK to disclose or divulge the same to Bidder in connection with the Services and the use and possession thereof by Bidder for or in connection with such purposes will not infringe any intellectual property rights of any third party. The BANK shall effectively indemnify, defend and hold Bidder harmless against all losses, damages, demands, costs or expenses which may be suffered or incurred by Bidder in connection with any such third party claim.</p>		
22	<p>Page No. 9 Clause No. 23 Liquidated Damages</p>	<p>The liquidated damages is an estimate of the loss or damage that the Bank may have suffered due to delay in performance or non-performance of any or all the obligations (under the terms and conditions of the purchase contract relating to supply, delivery, installation, operationalisation, implementation, training, support/services, acceptance, maintenance, etc., by the bidder/successful bidder and the bidder/successful bidder shall be liable to pay the Institute a fixed amount for each day of delay / nonperformance of the obligations by way of liquidated damages, details of which will be specified in the Tender. Without any prejudice to</p>	<p>We request bank to remove the mentioned clause as LD is covered under the delay in implementation clause</p>	<p>No change in the clause of bid document..</p>	<p>Page No. 9 Clause No. 27</p>

		<p>the Bank's other rights under the law, the Institute shall recover the liquidated damages, if any, accruing to the Bank, as above, from any amount payable to the Bidder either as per the tender, executed between the parties or under any other purchase agreement / contract, the Bank may have executed / shall be executing with the bidder/successful bidder.</p>		
23	NA	General : Legal	<p>Bidder suggests below additions 1. Limitation of Liability C-EDGE shall be excused and not be liable or responsible for any delay or failure to perform the services or failure of the services or a deliverable under this Agreement to the extent that such delay or failure has arisen as a result of any delay or failure by the CUSTOMER or its employees or agents or any third party service provider of the CUSTOMERs and their employees to perform any of its duties and obligations as set out in this Agreement. In such event, the C-EDGE shall be allowed an additional period of time to perform its obligations and unless otherwise agreed the additional period shall be equal to the amount of time for which C-EDGE is delayed or prevented from performing its obligations due to such failure or delay on the part of or on behalf of the CUSTOMER or its employees or agents or third party service providers of the CUSTOMER and their employees. Such failures or delays shall be brought to the notice the CUSTOMER and subject to mutual agreement with the CUSTOMER, the C-Edge shall take such actions as may be necessary to correct or</p>	<p>No change in the clause of bid document..</p>

			<p>remedy the failures or delays. Neither Party shall be liable for any indirect, special, incidental, exemplary or punitive damages (including, without limitation, loss of revenue, profits, business) under this agreement and the aggregate liability of Company, under this agreement shall not exceed more than the total fees actually received to the company from the Bank for the Service that gives rise to such liability during the twelve month period immediately preceding such claim.</p> <p>2. INTELLECTUAL PROPERTY RIGHTS</p> <p>2.1 The intellectual property rights and the ownership in all the tools, processes, software, utilities, and methodology including any C-EDGE proprietary products or components thereof used in the provision of Services and/or development of Deliverables hereunder and all new ideas, inventions, innovations, or developments exclusively conceived, developed or made by C-EDGE while providing Services (including without limitation, the development of such Deliverables) hereunder shall remain the sole and absolute property of C-EDGE, and C-EDGE shall continue to retain ownership rights as regards all intellectual property therein (“C-EDGE INTELLECTUAL Property”). C-EDGE shall grant in favor of the BANK a non-exclusive, non-transferable, enterprise paid up license to use the C-EDGE Intellectual Property provided that the rights of the Customer to use such C-EDGE Intellectual Property does not include the rights to (a) sell, lease, exchange, mortgage, pledge, license, sub license, assign or in any other</p>		
--	--	--	---	--	--

			<p>way convey, transfer or alienate the C-EDGE Intellectual Property in favor of any third person (either for commercial consideration or not (including by way of transmission), and/or (b) reverse compile or in any other way arrive at or attempt to arrive at the source code of the C-EDGE Intellectual Property. 2.2 The BANK acknowledges that C-EDGE provides consulting, implementation and development services to other clients/customers and agrees that nothing in this Agreement shall be deemed or construed to prevent C-EDGE from conducting such business or to develop, use and distribute works that perform functions the same as or similar to the Deliverables or work products either for itself or for its other clients subject to C-EDGE maintaining confidentiality of the BANK confidential information and C-EDGE's provision of same/similar Services to other clients of C-EDGE shall not violate terms of this Agreement and/or any of the BANK's intellectual property rights. 3. Termination: 3.1 Either party may terminate this Agreement at any time upon written notice forthwith if the other party commits a material breach of this Agreement which cannot be rectified or other party is engaged in corrupt & fraudulent practices in executing the contract or the other party does not perform the obligations & conditions of this contract satisfactorily despite notice of default in this regard or acts in a manner prejudicial to the interest of the other party and does not remedy such breach within 30 days of service of written notice by the party not in default. 3.2 Either party</p>		
--	--	--	---	--	--

			<p>may terminate this Agreement at any time upon furnishing a written notice of 30 days to the other party if insolvency proceedings, winding up or liquidation proceedings are instituted against the other party has commenced. 3.4 Either party may terminate this Agreement at any time upon furnishing a written notice of 30 days to the other party pursuant to a prolonged Force Majeure event.</p>		
24	Page No. 13 Annexure – II	15. If any endpoint is having more than three days older virus definition and if such endpoint tries to connect the network, then the solution must immediately install latest virus definition by connecting to the endpoint management server and blocking all connections to the other network resources like internet, intranet applications etc	Request bank to provide clarity on; 1. Is Internet accessible in Bank Network? 2. Anti Virus will be updated but will not be able to block network resources (To update need connectivity)	No change in the clause of bid document..	Page No. 12
25	Page No. 13 Annexure – II	17. 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.	As per bidder understanding the mentioned clause is applicable to anti-virus patches only? Request bank to provide clarity on the mentioned clause.	Clause is applicable to anti-virus patches.	Page No. 12
26	Page No. 14 Annexure – II	36. The Solution must have a layer of protection that enables organization to go on the offensive, lure attackers out of hiding, and reveal attacker intent and tactics via early visibility, so that the information can be used to enhance security posture.	Request bank to remove the mentioned clause.	Solution should have multi layers of Defense mechanism which help protect customer endpoints from Known-Bad as well as Unknown attacks.	Page No. 13
27	Page No. 14 Annexure – II	39. The solution should be in the leader's quadrant of latest Gartner Report for endpoint security.	Request bank to remove the mentioned clause.	The clause is dropped.	

28	NA	General	Request bank to share the location where banks anti-virus server is hosted.	KCCB Head Office Dharamshala	
2. QuickHeal Technologies Ltd.					
Sr No.	RFP No. & Page No	RFP Clause	Suggestion/Deviation/Remark	Consultant Remarks	Clauses in the Revised Document After Pre Bid
1	Page No. 12 Annexure – II	1. The Solution should provide multi-layer of protection into a singleagent - (AV, NIPS, HIPS, Memory Exploit Mitigation, Advance Machine Learning, Emulation capabilities, Behavioural Monitoring and protection, reputation lookup, application and device control & system lockdown)	As per our understanding the clause means - The Solution should provide multi-layer of protection into a single agent - (Which may include AV, NIPS, HIPS, Memory Exploit Mitigation, Advance Machine Learning, Emulation capabilities, Behavioural Monitoring and protection, reputation lookup, application and device control & system lockdown). Please confirm.	The Solution should provide multi-layer of protection into a single agent - (Which may include AV, NIPS, HIPS, Memory Exploit Mitigation, Advance Machine Learning, Emulation capabilities, Behavioural Monitoring and protection, reputation lookup, application and device control & system lockdown)	Page No. 11 Annexure – II
2	Page No. 12 Annexure – II	2. Network threat protection should analyse 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. Network threat protection should analyse 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.	As per our understanding the clause means - Solution Must have the capability to detect, and prevent network based and host based intruder attempts on the home networks. Solution Must have the capability to prevent port scanning attacks & capability to prevent DDOS attacks. Rules-based firewall and browser protection should be included to protect against web-based attacks. Please confirm	Your understanding about the point is correct and is acceptable.	Page No. 11 Annexure – II
3	Page No. 12 Annexure – II	4. Correlate different linkages between users, files, and websites to detect rapidly mutating threats. By analysing key	As per our understanding, the clause means "Solution must have signature-less, behavior-based, real-time engine designed to detect and stop	Solution must have signature-less, behavior-based, real-time engine designed to detect	Page No. 11 Annexure – II

		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. Correlate different linkages between users, files, and websites to detect rapidly mutating threats. By analysing 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.	new & unknown malware that tries to infect a user's computer. Analyses the structure of the software program, its programming logic or computer instructions, and other static attributes such as size, location etc and should be Effective against zero-day attacks. By analysing 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." Please confirm	and stop new & unknown malware that tries to infect a user's computer. Analyses the structure of the software program, its programming logic or computer instructions, and other static attributes such as size, location etc and should be Effective against zero-day attacks.	
4	Page No. 12 Annexure – II	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.	As per our understanding the clause means - "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 scan compressed files to reduce the risk of virus/malware entering the network. " please confirm	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 scan compressed files to reduce the risk of virus/malware entering the network	Page No. 11 Annexure – II
5	Page No. 12 Annexure – II	10. The solution should allow administrator to run custom scripts on their endpoints to verify and report compliance; quarantine location and peer-to-peer enforcement lockdown and isolate a noncompliant or infected system. The solution should allow administrator to run custom scripts on their endpoints to verify and report compliance; quarantine location and peer-to-peer enforcement lockdown and isolate a noncompliant or infected system.	As per this clause we understand - "Solution should must isolate end points automatically in case of infection and network attack, Provision for Self/Tamper Protection for Seqrite EPS files/folders." Please confirm	Your understanding about the point is correct and is acceptable.	Page No. 11 Annexure – II

6	Page No. 13 Annexure – II	11. 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.	As this is a banking environment we recomend this which will fullfill your requirement - "Solution must have capability to configure policies for roaming clients even if it is out of network through cloud based management platform and Must have capability to get status, reports from roaming clients even if it is out of network through cloud based management platform. Status should include endpoint name, host IP, MAC etc.". Please confirm	Solution must have capability to configure policies for roaming clients and to get status, reports from roaming clients even if it is out of network through cloud based management platform. Status should include endpoint name, host IP, MAC etc.	Page No. 12 Annexure – II
7	Page No. 13 Annexure – II	14. The solution should auto-compile, auto-protect when the operating system kernel is not compatible with precompiled auto-protect kernel module especially for Linux variants.	We recomend/ propose following for a Linux environment which is suitable in a End Point protection scenerio - " Must offer comprehensive client/server security for Linux Variants by protecting enterprise networks from viruses, Trojans, worms, hackers, network viruses, mixed threat attack from multiple entry points, and spyware. Must have the capability to scan external drives such as USB Storage, CD/DVD's. Must have capability to monitor and protected shared folders on Samba Server. Please consider and confirm	Must offer comprehensive client/server security for Linux Variants by protecting enterprise networks from viruses, Trojans, worms, hackers, network viruses, mixed threat attack from multiple entry points, and spyware. Must have the capability to scan external drives such as USB Storage, CD/DVD's. Must have capability to monitor and protected shared folders on Samba Server.	Page No. 12 Annexure – II
8	Page No. 13 Annexure – II	15. If any endpoint is having more than three days older virus definition and if such endpoint tries to connect the network, then the solution must immediatly install latest virus definition by connecting to the endpoint management server and blocking all connections to the other network resources like internet, intranet applications etcIf	As per our understanding, this clause means - "If any endpoint is having more than three days older virus definitionand if such endpoint tries to connect the network, then the solution must immediatly install latest virus definition by connecting to the endpoint management serverMay block all connections to the other network resources like internet, intranet applications	Your understanding about the point is correct and is acceptable.	Page No. 12 Annexure – II

		any endpoint is having more than three days older virus definition and if such endpoint tries to connect the network, then the solution must immediately install latest virus definition by connecting to the endpoint management server and blocking all connections to the other network resources like internet, intranet applications etc	etc. Also, if we configure only IP address and Subnet on network adapter then PC will not communicate with internet but will get update from LAN server (VDB Updates Only). Please confirm		
9	Page No. 13 Annexure – II	16. If the host is non-compliant with the policies, the solution must automatically initiate remedial action, which may include running isolating it from network, downloading and executing/inserting a software, running scripts, by setting required registries keys. The solution should recheck host for compliance after remediation and grant access for the compliant host to the network.If the host is non-compliant with the policies, the solution must automatically initiate remedial action, which may include running isolating it from network, downloading and executing/inserting a software, running scripts, by setting required registries keys. The solution should recheck host for compliance after remediation and grant access for the compliant host to the network.	As per our understanding this clause means - "If the host is non-compliant with the policies, the solution must automatically initiate remedial action, which may include running isolating it from network, downloading and executing/inserting a software, running scripts, by setting required registries keys.Solution must have capability to scan infected end point after remediation and push allowed polices. Solution should must have boot time scan capabilities". Please confirmAs per our understanding this clause means - "If the host is non-compliant with the policies, the solution must automatically initiate remedial action, which may include running isolating it from network, downloading and executing/inserting a software, running scripts, by setting required registries keys.Solution must have capability to scan infected end point after remediation and push allowed polices. Solution should must have boot time scan capabilities". Please confirm	Your understanding about the point is correct and is acceptable.	Page No. 12 Annexure – II
10	Page No. 13 Annexure – II	17. The solution must be able check whether required software, security patches and hot fixes have not been installed on the endpoint as mandated by	As per our understanding this clause means - "Solution Must have capability to scan missing patches for Microsoft applications. For example: Windows, Office, Internet	Your understanding about the point is correct and is acceptable.	Page No. 12 Annexure – II

		organization, the solution should be set to connect to an update server to download and install the required software based on the policy. 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.	Explorer along with missing patches for Non-Microsoft applications. ex: Adobe Reader, Adobe Acrobat, Adobe Flash Player, VLC, Java, Putty, Notepad++, 7-Zip, Mozilla Firefox and Mozilla Thunderbird. It should generate reports of missing patches as per client and must have capability to schedule scanning and installation of missing patches." Please confirm		
11	Page No. 13 Annexure – II	20. Must provide Real-time lock down of client configuration – allow or prevent users from changing settings or unloading/uninstalling the software	As per our understanding this clause means - "Solution should must have password based authentication for end points, capability to prevent a user from accessing the operating system in safe mode and tampering any services." Please confirm	Your understanding about the point is correct and is acceptable.	Page No. 12 Annexure – II
12	Page No. 13 Annexure – II	22. Solution should detect command and control traffic activity with IP level events, URL events, and DNS activity using detection mechanisms like static analysis, behavioral analysis, and reputation analysis from intelligence network.	As per our understanding this clause means - "Soulition should must have protection from signature and signature less attack along with browsing & phishing protection. Solution must be capable of threat hunting using AI/ML technologies". Please confirm	Your understanding about the point is correct and is acceptable.	Page No. 12 Annexure – II
13	Page No. 13 Annexure – II	23. 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 thresholdCPU usage performance control during scanning: 1) Checks the CPU usage level configured on the	Our solution allows Administrators to define the 'Priority' feature (Low, Normal or High) to set the scan priority of the scan features based on need which is directly linked to CPU utilization. So we request you to please option for scan priority configuration as well. Our solution allows Administrators to define the 'Priority' feature (Low, Normal or High) to set the scan priority of the scan features based on need which is directly linked to CPU utilization. So we request you	Option for scan priority configuration is accepted.	Page No. 12 Annexure – II

		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	to please option for scan priority configuration as well.		
14	Page No. 14 Annexure – II	25. 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	Request you to please amend this clause as - "Solution may 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"	Clause modified as : Solution may 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"	Page No. 13 Annexure – II
15	Page No. 14 Annexure – II	30. Solution should provide anomaly detection to detect and report on suspicious information found in a file. Preferable capabilities should include, TLS call-back activity, CVE and exploit detection, shell-code detection, debugger detection, watermark tampering, and nonstandard file alignment, RFC compliant etc	As per our understanding this clause means - "Solution must have capabilities to scan the known vulnerabilities in the installed applications of various vendors such as; Adobe, Apple, Mozilla, Oracle etc. and the operating systems on the endpoints in your network and assess their security status. Must have solution for Important Vulnerability which may result in compromise of the confidentiality, integrity, or availability of user data." Please clarify	Your understanding about the point is correct and is acceptable.	Page No. 13 Annexure – II
16	Page No. 14 Annexure – II	31. 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.	Request you to please amend this clause as - "The solution may set up peer-to-peer authentication policy, which can grant or block inbound access to the remote computers that have the client installed." Please confirm	Clause modified as "The solution may set up peer-to-peer authentication policy, which can grant or block inbound access to the remote computers that have the client installed."	Page No. 13 Annexure – II
17	Page No. 14 Annexure – II	36. The Solution must have a layer of protection that enables organization to go on the offensive, lure	We propose to amend this clause as "Solution should have multi layers of Defense mechanism which help protect	Clause amended as: "Solution should have multi layers of Defense	Page No. 13 Annexure – II

		attackers out of hiding, and reveal attacker intent and tactics via early visibility, so that the information can be used to enhance security posture.	customer endpoints from Known-Bad as well as Unknown attacks." Please confirm	mechanism which help protect customer endpoints from Known-Bad as well as Unknown attacks."	
18	Page No. 14 Annexure – II	39. The solution should be in the leader's quadrant of latest Gartner Report for endpoint security.	We request you to kindly remove this clause as per recommendation from Ministry of Commerce vide letter dated 20/06/2019 (restrictive and discriminatory Condition). letter attached for your reference	The Clause is deleted	
3. K7.					
Sr No.	RFP Page No. & Clause No	RFP Clause	Suggestion/Deviation/Remark	Consultant Remarks	Clauses in the Revised Document After Pre Bid
1	Page No. 12 Annexure – II	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)	System lockdown feature not available in our EPS right now. Rest OK	The Solution should provide multi-layer of protection into a single agent - (Which may include AV, NIPS, HIPS, Memory Exploit Mitigation, Advance Machine Learning, Emulation capabilities, Behavioural Monitoring and protection, reputation lookup, application and device control & system lockdown)	Page No. 11 Annexure – II
2	Page No. 12 Annexure – II	10. The solution should allow administrator to run custom scripts on their endpoints to verify and report compliance; quarantine location and peer-to-peer enforcement lockdown and isolate a non-compliant or infected system.		Query of Self Isolation method, either can do automatic or manual.	Page No. 11 Annexure – II
3	Page No. 13 Annexure – II	11. The solution should automatically detects what location a system is	K7 Endpoint Security can automatically detect the location and apply the	Query of Self Isolation method, either can do	Page No. 12 Annexure – II

		connecting from, such as a hotspot, wireless network, or VPN and adjusts the security to offer the best protection for the environment.	appropriate policies as per the configuration of In-Office and Out-Office Firewall Rules.	automatic or manual.	
4	Page No. 13 Annexure – II	14. The solution should auto-compile, auto-protect when the operating system kernel is not compatible with precompiled auto-protect kernel module especially for Linux variants.	We don't support Linux platform as of now. But it is in pipeline.	Linux support is required as per RFP.	Page No. 12 Annexure – II
5	Page No. 13 Annexure – II	23. 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	Not required. Solution uses least resources when compared with any other solution in the market	No comments	Page No. 12 Annexure – II
6	Page No. 14 Annexure – II	27. The solution should manage single license for windows, Linux and mac Operating Systems and management server should not be separate.	We don't support Linux & MAC platform as of now. But it is in pipeline. We have standalone solution for MAC.	Linux support is required as per RFP, however Mac support is relaxed.	Page No. 13 Annexure – II
7	Page No. 14 Annexure – II	32. The Solution should provide manage windows, Linux and mac agents from same centralized console.	We don't support Linux & MAC platform as of now. But it is in pipeline. We have standalone solution for MAC.	Linux support is required as per RFP, however Mac support is relaxed.	Page No. 13 Annexure – II
8	Page No. 14 Annexure – II	36. The Solution must have a layer of protection that enables organization to go on the offensive, lure attackers out of hiding, and reveal attacker intent and tactics via early visibility, so that the information can be used to enhance security posture.	K7 deliver powerful multi-layer protection with AI Enhanced latest cyber security software to protect your computer data.	Solution should have multi layers of Defense mechanism which help protect customer endpoints from Known-Bad as well as Unknown attacks	Page No. 13 Annexure – II
9	Page No. 14 Annexure – II	39. The solution should be in the leader's quadrant of latest Gartner Report for	Public Procurement (Preference to Make in India) Order 2019 for Cyber Security Products	The clause is dropped.	

		endpoint security.	https://www.meity.gov.in/write/readdata/files/public_procurement-preference_to_make_in_india-order_2019_for_cyber_security_products.pdf		
--	--	--------------------	---	--	--

4. Accel IT Services.

Sr No.	RFP No. & Page No.	RFP Clause	Suggestion/Deviation/Remark	Consultant Remarks	Clauses in the Revised Document After Pre Bid
1	Page No. 3 Clause No. 6(3)	Should have experience in the following fields: Supply and Installation of Enterprise Anti[1]Virus / Endpoint Security Software License for government and financial organizations	Should have experience in the following fields: Supply and Installation of Enterprise Anti[1]Virus / Endpoint Security Software License or AMC Support for government or private institution or financial organizations.	Not accepted	Page No. 3 Clause No. 6(3)
2	Page No. 3 Clause No. 6(8)	8. The Bidder shall provide references (including Referee names and contact details) in respect of major projects of similar type completed in the last Three(3) years by the Bidder in any large organization and having its offices/branches across India.	The Bidder shall provide references (including Referee names and contact details) in respect of major customer to who providing satisfactory IT support during last (3) years by the Bidder in any large organization. Satisfactory letter to be attached.	As per RFP	Page No. 3 Clause No. 6(8)

5. Team Computers Pvt. Ltd.

Sr No.	RFP No. & Page No.	RFP Clause	Suggestion/Deviation/Remark	Consultant Remarks	Clauses in the Revised Document After Pre Bid
1		Share Plan to Upgrade XP machine as most of the OEMs are not supporting XP.		Tender in Process	
2		Bank should go for AV along with EDR that will create strong protection.		Not accepted	