BIMAN BANGLADESH AIRLINES LTD.
PROCUREMENT & LOGISTIC SUPPORT DIRECTORATE
LOCAL PURCHASE SECTION
BIMAN ADMIN. BLDG. HAZRAT SHAHJALAL INTERNATIONAL AIRPORT, DHAKA
FAX: 880-2-8913028, PH: 8901325 & 8901500-19/EXT:4226 & 4220

TENDER NO: Re-OTM No:118/2020-21 **DATE:** 28/07/2021

DATE & TIME OF CLOSING: 17/08/2021 AT 1100 HRS (LT)

DATE & TIME OF OPENING: 17/08/2021 AT 1400 HRS (LT)

PRICE: BDT.1,000.00 (One thousand) only (Non-refundable).

M/S---------- CR.NO----------DATE----------

---------- SIGNATURE----------

STAFF/NO----------

Tender in sealed envelope is hereby invited from interested Manufacturer's Authorized Partner for 03 years duration License Renewal of **Endpoint Protection System** belongs to Biman Bangladesh Airlines Ltd.

01. Technical Compliances

Endpoint Security Solution with Zero-day Protection	
Sl. No	Features
1	Single Agent: Should be a single agent that combines all the critical components for comprehensive security on the endpoint. (Antivirus, Antispyware, devicecontrol, desktop firewall, Desktop HIPS, application control, encryption etc.)
2	It should be managed from a single centralized management console which should provide Instant visibility into the security state and health of endpointsecurity products and not based on logs. Real-time actions help ensure that defenses are installed, running, correctly configured, and up to date.
3	Heuristic virus scan: Should Scan files and identifies infections based on behavioral characteristic of viruses
4	On-access virus scan :Should Scan files as they are opened, executed, or closed, allowing immediate detection and treatment of viruses
5	Scan target drives: Should specify directories and file types to scan
6	Scan exclusions: Should specify directories and file extensions not to be scanned

Continued Page-02

7	Should have Configurable Scanning. Should have the ability to control the amount of CPU resources dedicated to a scan process
8	Treatment options: Should Enable choice of action agent should take upon detection of virus: Repair, rename, quarantine, delete
9	Intelligent quick scan: Should Check the most common areas of the file system and registry for traces of spyware
10	Should support unique real time update based on over the web cloud technology to provide real time signatures for dynamic and latest threats to reduce thedependency on Daily Signature updates.
11	Should have a different protection level in cloud based intelligence. This includes Very Low, Low, Medium, High and Very High.
12	Full-system scan: Should Scans local file folders and specific file types
13	Should be able to lock down all anti-virus configurations on the system
14	User should be prevented from being able to uninstall the anti-virus software.
15	Must be able to totally protect from spyware, adware, Trojans, key loggers, P2P Threats, Hackers tools, DDOS Attack Agents, in real time
16	Should have centralized management and reporting capabilities to deliver reports like top Spywares, by category, by infected machines, by risk priority etc.
17	Real time Active protection on memory, process termination / file removal of pests in active memory
18	Should have centralized update/download mechanism which should be able to download details of latest Spywares and push the same across all the desktops
19	The solution must be able to auto-quarantine or auto-delete spyware or adware without end-user interaction
20	Browser Security : Should Support Internet Explorer 6, 7, 8,Mozilla Firefox 2, 3
21	Proposed solution should have integrated URL categorization feature
22	Proposed solution should categories URLs for threats like – Spywares, Trojans, Spam, Adware etc.
23	Solution URL category module should provide end user detail threat information about the site
24	Should be able to update definitions & scan engine on the fly, without a need for reboot or stopping of services on servers.
25	Solution should provide real time cloud based intelligence to detect newer threats.
26	The solution should be able to determine file-execution decisions with rule-based logic based on endpoint context (file, process, and environmental attributes)blended with collective threat intelligence.

Continued Page-03

27	The proposed solution should be able to map the global intelligence from their own cloud with the local intelligence collected from endpoint solution proposed.
28	The proposed endpoint protection solution should be able to integrate with third party feeds such as Virus Total in the same endpoint management console.
29	The proposed endpoint protection solution should be able to import threat reputation of files through file hashes into the central endpoint protectionmanagement solution.
30	The proposed endpoint solution should be able to automatically prevent the execution of even unknown executable files even if the endpoint does not havethe latest signatures and without heuristics or behavioral patterns.
31	Should not block just on file hashes but on certificate bases also such that only trusted certificates are allowed to execute.
32	The solution should provide an Integrated firewall which should use reputation scores based on vendors global threat intelligence to protect endpoints frombotnets, DDoS, APTs, and suspicious web connections.
33	The proposed solution should provide an option for the administrator to pick and choose the protection modules they want for their endpoints based on theirsystem type and environment.
34	The solution should have an integrated endpoint-assisted security installation (EASI) installer to offer an accelerated and simplified deployment process.
35	The proposed endpoint security solution should be able to undertake pre-execution analysis for unknown malware while performing Static file featureextraction (for example file type, import hash, entry point, resources, strings, packer & compiler details, compile time, API's, section names etc.)
36	The proposed endpoint security solution should be able to undertake Post-execution analysis for unknown malware while performing Behavioral featuresand Memory analysis (for example behavioral sequence, process tree, file system, registry events, network communication events, mutex, strings from memory etc.)
37	The proposed solution should be able to quarantine and contain unknown malware samples on endpoints especially malware which can evade sandboxanalysis
38	The proposed endpoint security solution should Extract static file feature for classification by using a machine learning model that resides on endpoint andthe Static feature based detection should not require cloud lookups.

Continued Page-04

39	The proposed endpoint security solution should provide the ability to Traces program execution events (file system, registry and network events) using light-weight client on the endpoint and should leverages both static properties of thefile and runtime execution trace of files as features for real-time behavioral classification.
40	The solution should potentially block the end point system from loading physical devices such as removable storage devices, Bluetooth, Wi-Fi, and other plug andplay devices based on device classes and device definitions are used to define device rules
41	It should support device management and should allow you to Monitor, Block or make the device Read-Only along with the option of providing exceptions
42	It should support for detecting attempts to copy confidential data to removable storage devices (e.g. USB drives, floppy, CD/DVD, etc.).
43	It should support for blocking Windows native CD writing and other CD writing software. The block must inform the user that the action is being blocked.
44	It should support for customizable notification "pop-up" messages
45	It should be able to control the access of USB devices by using their vendor ID, product ID or serial number.
46	The solution installation, policy management and reporting should be handled by an integrated endpoint agent on the client.
47	he solution should provide near real-time event monitor allowing you to see events as they happen, view details (user, machine, rules triggered, etc), andeven access evidence files as the events happen in your environment.
48	It should support ability to restrict access to company approved devices, but also if necessary to permit exclusions to this requirement. Exception and/orexclusions can be designed to accommodate different devices or different groups of users
49	It should provide the functionality of logging and audit-trail capabilities
50	It should support Signature as well as behavioral based detection
51	It should support policies creation based on – User defined, Adaptive mode and Learn mode
52	It should support desktop firewall capabilities to directly block unwanted traffic
53	HIPS solution should provide facility to create different policy for different network connectivity like – LAN, DHCP.
54	It should support firewall policy to enable cloud based network reputation lookup. For e.g. if a client is communicating with an IP address with a badreputation or bad URL, the firewall should stop the communication withouthaving to create a rule.

Continued Page-05

55	HIPS Solution should provide blocking of unwanted applications trying to run
56	HIPS solution should provide facility to create User defined signatures
57	HIPS solution should provide protection from known attacks like – SQL injection, Cross Site scripting, Buffer Overflow without having signatureupdates
58	HIPS solution should provide vulnerability shielding to the application not having patches installed
59	The Solution should ensure that Only authorized software / applications / executable codes are allowed to run and provides tamper protection to them.
60	Solution should be capable of creating white list for each system dynamically and no manual intervention in creating this list.
61	Each white list created should be unique to each system and should not be a common list
62	The solution should emper the user to self-approve any new application / software with business justification. So that new application can be run successfully with notification to administrator.
63	Solution should allow administrator to approve or revoke self-approved application status so that new application can be allowed to run or ban.
64	Solution should consider executables, activeX, Java, Perl scripts, bat files, VBS files, com files, dll files, sys files while creating the white list.
65	Solution should be capable of locking down the system on the white list created above and prevent execution of nonwhite listed software / application /executable code.
66	Solution should prevent tampering of applications which are white listed above either on disk or on memory when running
67	The Solution should have the capability to run on observation mode post white list creation so that new applications / software's / codes are not stopped fromrunning but are monitored only. If required administrator should be able to approve or revert back to base line.
68	The Proposed solution should support Manual submission for analysis
69	Endpoint APT solution should have the option to send the file to sandbox for theanalysis and can take the action based on result.
70	The proposed solution should be able to detect and prevent advance targetedmalware in the endpoint infrastructure.
71	The proposed endpoint advance malware analysis solution should be able tointegrate with third party feeds in the same endpoint management console.
72	The proposed endpoint advance malware analysis solution should be able toimport threat reputation of files through file hashes into the central management solution.

Continued Page-06

73	The proposed endpoint advance malware analysis solution should be able to automatically prevent the execution of even unknown executable files even ifthe endpoint does not have the latest signatures and without heuristics or behavioral patterns.
74	Solution should Capture and monitor context and system state for changes that may be IoCs, as well as find dormant attack components, and send intelligence toanalytics, operations, and forensic teams
75	Solution should have capability to search on any file or IOC's generated by APT solution centrally and should have capability to hunt in entire organization wideendpoints and correct/remediate centrally.
76	The proposed ability to destroy undetonated malicious executables within theenvironment with the ability to hunt for such malicious executables
77	Endpoint security solution should have Machine learning and Ransomwareprotection module to protect endpoints from attacks.
78	Solutions should support report customization and allow viewing directly using a web browser and also as a dashboard using the same management console forthe endpoints.
79	Solution should supports the following formats for exporting data: CSV, HTML, XML, Acrobat PDF,
80	Solution should support ability to restrict access to company approved devices, but also if necessary to permit exclusions to this requirement. Exception and/orexclusions can be designed to accommodate different devices or different groups of users
81	Solution should provide the functionality of events being viewed, filtered, and sorted in the Management console, allowing security officers or administrators to view events and respond quickly. If applicable, suspicious content is attachedas evidence to the event.
82	Solution should provide the functionality of logging and audit-trail capabilities.
83	Solution should provide the capability to log administrative activities in the Management console. Administrative activities that are logged in the Management console include, changes to policies, deployment of policies, agentoverride activities, agent termination, and agent uninstall key generation.
84	Qty/Users: 899, For Server: 10
85	Brand: To be mentioned by the bidder Product/Version: To be mentioned by the bidder

Continued Page-07

Server Security Solutions	
1	The solution should offer Application Control, Change Control, HIPS, and Virtualized Security functionality to ensure optimal security and compliance forcritical servers.
2	The solution should be managed from a single centralized console.
3	The solution should have a small overhead footprint such that it minimizes impact on system resource
4	The proposed solution shall support the following Server platforms - Windows 2008 Server - Windows 2012 Server - Windows 2016 Server - Red Hat Linux - Solaris - AIX - CentOS
5	The solution should provide the dynamic management of execution capability of applications on a server system, prevent unauthorized registry manipulationand in memory protection of application
6	The solution should be able to enforce a server system in a "gold image" as decided by the system administrator.
7	It should prevent execution of all unauthorized software, scripts, and dynamic-link libraries (DLLs) and further defends against memory exploits
8	The solution should provide for a real time capability to prevent execution of any authorized application to execute on the server system
9	The solution should allow an administrator to authorize a well-defined update mechanism to alter the state of gold image as being enforced currently to a newgold image.
10	The solution should allow an administrator to remote view the constituents of a system image and hence compare the image with a well-defined gold image.
11	In the absence of a gold image, the solution should provide for the capability to enforce a current good state as decided by the system administrator.
12	The solution should allow for well-defined update mechanism to allow changes to the state of server system and then enforce the new state of the system
13	The solution should not require updates to be rolled to client system in order to approve new applications to be executed.
14	The solution should allow/ban individual application based on different characteristics such as name, checksum etc.

Continued Page-08

15	It should restrict administrators with physical or remote access to the machine to override protection
16	The solution should augment blacklisting, real-time reputation awareness, and behavioral approaches, helping IT to consistently enable the known good, blockthe known bad, and properly handle the new and unknown.
17	The solution should prevent the tampering of application on the disk and in the memory.
18	The solution should have a small overhead footprint which includes:
19	Easy setup and low initial and ongoing operational overhead
20	No file system scanning that could impact system performance
21	Designed to work in disconnected and in “offline“ mode if necessary
22	The solution should be able to create inventory of a target system and hence report on installed software and applications on client machines.
23	The solution should not be dependent on any external verification of allowed/banned application. It should be able to take its input on the basis oflocal state of server system as verified by the system administrator
24	The solution apart from allowing only authorized applications to run, should block any changes from being done to authorized applications, like DLL's,System files, registry etc., thus providing application treat protection
25	The solution should support Real-time Change Tracking Audit log. It should Include File, User, Program name and contents that have changed
26	The solution should support Change Prevention as part of the core solution
27	The solution in the event of unauthorized file change, should reports WHAT changed, WHO made the change, HOW they made it and precisely WHEN theydid the changes
28	The solution should offer intelligent filters which are pre-configured to track the relevant objects on the system, for each standard Operating System covering systems files including Windows, Solaris, and Linux. It should alsoinclude application filters for Apache, Tomcat, WebSphere and JBOSS, IIS, WebLogic, WebSphere , etc., and should be customizable.
29	The solution should monitor application and operating system files in real time
30	The solution should provide email and SNMP alerts
31	The solution should integrate with change management, data center automation, and configuration management database (CMDB) solutions from HP, BMC, IBM,and others

Continued Page-09

32	The solution should be capable of tracking changes to databases in two manners (1) changes to the database structures themselves (tables, indexes etc.) (2)changes to the data itself, in real time
33	Solution must provide automated and centralized download and deployment of latest virus signature updates from the Internet to desktops and servers acrossthe organization, across different Windows platforms. Updates should be incremental with update sizes of ~100KB on average
34	Solution must provide flexibility to install different components (Like – Management Agent, AV client, Anti-Spyware, HIPS,) separately for better use ofnetwork bandwidth
35	Should have the ability to detect and remove unwanted programs, toolbars, adware, spyware, dialers etc & Post detection the actions that the antiviral performs must be the following: Alert / Notify , Clean, Delete / Remove, Move /Quarantine, Prompt for Action
36	Shall support multiple platforms – Windows 2012 ((Professional / Server /Advanced Server) / 2008 (Standard / Enterprise Edition) / Linux
37	Should support file scan caching to avoid repetitive scanning of files which are unchanged since the previous scan
38	Proposed solution must automatically scan Floppy disks, Compact disks, USB devices and Network shares in real-time when accessed.
39	Proposed solution should provide multiple policies to lockdown the server like –change in registry, Internet Explorer file settings, Exe file execution etc. to blockunknown zero day attacks and reduce dependency on frequent signatures
40	Should allow the On Demand Scanner to recognize the last scanned file and resume scanning from that file if an “On demand Scan” is interrupted
41	Should have the ability to control the amount of CPU resources dedicated to a scan process
42	The proposed solution should be capable of detecting and preventing buffer overflow vulnerability, irrespective of the exploit that is using the buffer overflow vulnerability. The solution should support buffer overflow detection and prevention on the following minimum applications: Windows OS Services,Media Player, Internet Explorer, SQL Server, Word, Excel, Power Point, Auto Update, Explorer, Instant Messenger, Outlook, Outlook Express etc
43	Proposed solution should be capable of blocking TCP/IP ports on the System and also creating exceptions for specified applications to use these blockedports.
44	Proposed solution should be capable of blocking read, write, execute, delete & change permissions on specified file(s)/folder(s)/Network Share(s).

Continued Page-10

45	Discover and Report the IP Address of the end-point system (infection source) that sent malicious code to the server and optionally, block further communications from the infection source end-point system for a configurabletime period or indefinitely
46	The proposed solution should provide Self-protection from modifying or disabling Antivirus Client
47	The proposed solution should scan system memory for installed rootkits, hidden processes, and other behavior that suggests malicious code is attempting to hideitself.
48	Proposed solution should allow to configure different policies for different set of Processes
49	The Antivirus should allow for automated rollback of virus definition, if required
50	Should be able to lock down all anti-virus configurations at the servers.
51	Proposed solution should be capable of detecting and blocking communication from hosts that are spreading viruses/worms.
52	Should support unique real time update based on over the web cloud technology to provide real time signatures for dynamic and latest threats to reduce thedependency on Daily Signature updates
53	have enhanced tamper protection that guards against unauthorized access and attacks, protecting users from viruses that attempt to disable security measures
54	It should support Signature as well as behavioral based detection
55	It should support policies creation based on – User defined, Adaptive mode and Learn mode
56	It should support desktop firewall capabilities to directly block unwanted traffic
57	HIPS solution should provide facility to create different policy for different network connectivity like – LAN, DHCP.
58	It should support firewall policy to enable cloud based network reputation lookup. For e.g. if a client is communicating with an IP address with a badreputation or bad URL, the firewall should stop the communication withouthaving to create a rule.
59	HIPS Solution should provide blocking of unwanted applications trying to run
60	HIPS solution should provide facility to create User defined signatures
61	HIPS solution should provide protection from known attacks like – SQL injection, Cross Site scripting, Buffer Overflow without having signatureupdates
62	HIPS solution should provide vulnerability shielding to the application not having patches installed

Continued Page-11

63	The Solution should allow encryption of complete hard drive sector by sector.
64	The product should support encryption of extended partitions. The configuration for full disk encryption is controlled from the management console by selecting the drive letter that you intend to encrypt regardless of thepartition type.
65	The Solution should provide Pre-Boot Authentication. With Pre-Boot Authentication enabled, only users that have been assigned to the asset(s) through the management console have access to authenticate post BIOS post.
66	The Product should allow the administrator to customize the Pre-Boot environment to tailor the UI to, for example, corporate graphics and/or custommessages.
67	The product should record the encryption status of each hard drive.
68	The Solution should support for reports to be exported to other formats like XML, CSV, HTML and PDF.
69	The Solution should support for multifactor authentication, including: smart-cards, biometrics, and RSA tokens for the use in end user authentication.
70	The product should provide a Single Sign-on Capability.
71	The product should provide any form of password synchronization with domains, or to simplify having accounts on multiple machines
72	The Product should provide information such as what all machines are encrypted, not encrypted, Fully encrypted or partially encrypted.
73	The Proposed Solution should offloads scanning, configuration, and DAT update operations from individual guest images to an offload scan server withinthe premises
74	The solution should build and maintain a global cache of scanned files to ensure that once a file is scanned and confirmed to be clean, subsequent VMs accessingthe file won't have to wait for a scan.
75	Should allow separate policies for on-access and on-demand scanning to enable fine-tuned security execution
76	Should provide Connector for VMware vSphere provides a complete view into virtual data centers and populates key properties such as servers, hypervisors,and VMs through the same management console.
77	The Solution should provide administrators gain visibility into the security status of all VMs and can monitor hypervisor-to-VM relationships in near realtime.
78	Antivirus for Storage should be built in with the solution to secure the storageenvironment and prevent the spread of Malware throughout the environment and network.
79	Solution should extend visibility and control across Amazon Web Services (AWS)and Microsoft Azure public clouds and physical servers.

Continued Page-12

Management	
1	The solution should be able to manage endpoint security, application control, change control Anti-Virus solution, Encryption from a single managementconsole
2	The management console should be web-based
3	It should be able to deploy, manage, and update agents and policies from one management platform.
4	The management console should support hierarchical grouping of machines and policy deployment. The grouping could be based on IP Address of a subnet ofmachines or a particular site.
5	The management console should supports use of Active Directory accounts and groups to manage roles
6	The management console should support granular role based access control
7	The management console should be able to automatically report about the new unprotected system connecting on the network
8	The management console should provide automatic generation and delivery of reports for the respective administrators
9	The management console should provide actionable reports
10	The management console should provide Reports in CSV, HTML,PDF and Excel Format
11	The solution should be able integrate with third party ticket management Solution
Vendors Eligibility Criteria	
1	Vendor should have experience of deploying 1000+ endpoint solution in any local Organization. Proof of Experience such as (soft copy of PO / Experiencecertificate) need to be submitted.
2	Vendor should have at least 3 Principle certified local technical expertise to deploy the solution and for troubleshooting as well.
3	Vendor must have at least 5 customer base with 1000+ endpoints local deployment.
4	Proposed solution offered from OEM must be rated as 'Leaders' or 'Visionaries'in the latest Magic Quadrant for Endpoint Protection published by Gartner

02. Bidder's Eligibility:

The Bidder must submit Tender along with the following documents:

a. Signed/initialled and stamped in each page of the tender document by the authorized signatory;

b. Valid trade license;

c. Valid TIN Certificate and tax return certificate/Tax Submission document for current year;

d. Valid VAT Registration certificate;

e. Manufacturer's Authorization Letter;

f. Original Tender Schedule must be submitted with signature and seal of tenderer in every page along with original copy of schedule purchased money receipt (CR).

Continued Page-13

03. Delivery Schedule: The Bidder must complete the activities within 07 (seven) working days from issuance of purchase order.

04. Other Terms & Conditions:

a. The bidders must quote the cost both in figure and words including VAT, Taxes and Others. The Offer must be made in BDT (Bangladeshi Taka).

b. Biman reserves the right to accept or reject any or all the quotations without arising any reasons whatsoever.

c. If the bidder submits any wrong information then Biman reserves the right to reject their quotation partially or fully.

d. After successfully completion of the license renewal, Bill will have to be submitted and processed.

e. If the bidder fails to configure the proposed solution in Biman environment or successfully doesn't run, the purchase order will be cancelled with forfeiting the performance security money.

05. Earnest money (Refundable) for Tk.27,000/- (Twenty seven thousand) only in the shape of PO/DD/BG in favour of 'Biman Bangladesh Airlines Ltd.' must be submitted along with the offer from any schedule bank of Bangladesh. Earnest Money shall be refunded to the unsuccessful bidder as convenience of Biman.

06. Any Overwriting/erasing in the tender shall not be accepted unless properly countersigned by the Authorized person of the bidder.

07. Tender in sealed covers shall be received in Local Purchase Section, Procurement & Logistic Support Directorate, Biman, Hazrat Shahjalal International Airport, Dhaka and also in Biman Balaka Bhaban, Security Counter (Ground Floor), Dhaka latest by 1100 Hrs (BST) on **17/08/2021.** Offer shall be opened on the same day in the Tender Room, Biman Admin. Building, 1st floor, Procurement & Logistic Support Directorate, Biman, Hazrat Shahjalal International Airport, Dhaka in presence of the representative(s)/ Tenderer's (if any) at 1400 Hrs (BST).

08. Any Tender received after aforesaid specified date and time shall not be entertained. Biman will not bear any responsibility for late receipt of tender due any postal irregularities or otherwise.

09. Offer shall remain valid for 120 (One hundred twenty) days from the date of tender opening.

10. All submitted documents must be numerically serial showing total number of sheets and each sheet must be sealed and signed.

11. Performance Guarantee @10% on total value (Refundable) in the shape of PO/DD/Bank Guarantee to be submitted by the successful bidder within 07 days from the date of receipt of the notice for award of the contract/purchase order, in favour of 'Biman Bangladesh Airlines Ltd.' from any schedule bank of Bangladesh for a period of minimum 3½ year for the items. For Bank Guarantee it must have validity from the date of issuance of the guarantee till the required period. Earnest Money may be refunded upon receipt of Performance Guarantee. The purchaser reserves the right to encash/forfeits the Performance Guarantee in the event of failure of the supplier to complete the work. If the successful bidder fails to submit Performance Guarantee within the stipulated time, his Earnest Money will be forfeited.

Continued Page-14

12. Only unconditional offer will be accepted.

13. **TENDER SHALL BE REJECTED IF ANY OF THE ABOVE TERMS AND CONDITIONS ARE NOT FULFILLED**.

14. Completion of the work must be accompanied by 02 copies of supplier's challan showing description, quantity, packing list etc. addressing to: Manager (Commercial Store), P & L S Directorate, Biman, HSIA, Dhaka. The inspection and tests shall be conducted at the Biman Information Technical Unit (IT Unit), Balaka Bhaban, HSIA, Dhaka. If the work/service is rejected by the Inspection Committee, it must be completed within 01 (one) week (L/D charge shall be applicable if delivery schedule exceed) at suppliers risk and expenses.

15. The liquidated damages (L/D charge) will be paid by the supplier at the rate of 02% of the contract value per month or part of a month.

16. Undersigned may be contracted for any clarification during office hours on all working days.

17. Biman Bangladesh Airlines Ltd. reserves the right either to accept or reject any or all Tenders without assigning any reason thereof.

Manager (Commercial Purchase)
Phone: 8901325

I/We.....M/s..... owner/
representative hereby declare that I/We have accepted all Terms and Conditions of Tender papers and submitted quotation accordingly.

Signature: ---------- Date: ----------

Seal: ---------- Address: ----------

Phone/Mobile:---------- Fax: ----------Email: ----------