Meghalaya
Information Technology Society

NIC Building, Secretariat Hill, Shillong 793 001

No.MITS.2/2017/Pt/46 Dated Shillong the 25th June, 2020

REVISED NOTICE INVITING TENDER

Online bids are invited in two cover bid system, i.e. technical and financial bids separately from the authorized Original Equipment Manufacturers (O.E.Ms.), Authorized Distributors/ Authorised Dealers/Suppliers for "Supply and Installation of the IT Equipment and Software at Meghalaya State Data Center". The tender document details are available at state e-procurement portal @ https://meghalayatenders.gov.in. This revised tender supersedes the previous Tender No. MITS.2/2017/Pt/04 dated Shillong the 3rd June, 2020 and its corrigendum and addendum No. MITS.2/2017/Pt/38 dated Shillong the 19th June, 2020.

Sd/-

(K. L. Nongbri)
Joint Secretary to the Govt. of Meghalaya
Information Technology & Communications Department
&
Member Secretary
Meghalaya IT Society

Meghalaya
Information Technology Society

NIC Building, Secretariat Hill, Shillong 793 001

REVISED RFP/TENDER FOR SUPPLY AND INSTALLATION OF IT EQUIPMENT AND SOFTWARE FOR THE MEGHALAYA STATE DATA CENTER

Brief details of Revised RFP /Tender:

Tender Reference No.	No.MITS.2/2017/Pt/46 Dt. 25th June, 2020
Name of Organization	Meghalaya Information Technology Society (MITS), Shillong.
Tender Type	Open
Tender Category	Goods
Type / Form of Contract	Supply and Installation/commission
Product Category	Information Technology
Payment mode	Offline
Currency	INR
Bid submission last date	6th July, 2020 @ 5:00 PM
Date and time of Opening of Technical Bid through Video Conferencing	7th July, 2020 @ 3:00 P.M.
Date and time of Opening of Financial Bid	To be announced after Technical bid evaluation
Tender Fees (Non-refundable)	Rs 1000.00
Number of Covers 2 **Technical Bid** (eligibility criteria and technical specifications) + **Financial Bid**	**MSME & SINGLE POINT NSIC registered vendor are exempted from payment of EMD.**
Bid Validity days	90

1. OBJECTIVE / SCOPE

The scope of the tender is for "Supply and Installation of the IT Equipment and Software at Meghalaya State Data Center", Shillong.

2. ELIGIBILITY CRITERIA:

a. Eligibility Criteria is given in **ANNEXURE- I: ELIGIBILITY CRITERIA - CHECKLIST"**
b. Documentary evidence for compliance to each of the eligibility criterion must be enclosed along with the bid.

3. EARNEST MONEY DEPOSIT:

a) Earnest Money Deposit (EMD) of Rs.50,000/- (Rupees Fifty Thousand only) in the form of BG/DD from any commercial banks in favour of Member Secretary, Meghalaya IT Society, Shillong.
b) The Earnest Money Deposit (EMD), without any interest accrued will be refunded as follows:
    i. In the case of those Bidders who failed to qualify during the technical

bids, the Earnest Money Deposit (EMD) will be refunded without any interest accrued within one month of the acceptance of Technical Bid.

ii. In the case of those Bidders who are not awarded the contract, the Earnest Money Deposit (EMD) will be refunded without any interest accrued within one month of the acceptance of Financial Bid.

iii. In the case of Bidders whose tender bids are accepted for supply, EMD will be refunded on receipt of **Performance Security Deposit** as per award of contract clause.

In the case of Bidders whose tender bids are accepted for supply, EMD will be refunded on receipt of Performance Bank Guarantee (PBG) **which is 10% of the Contract Value** *for hardware items only in the form of Bank Guarantee in favour of Member Secretary, Meghalaya Information Technology Society (MITS), Shillong is to be submitted to MITS* as per award of contract clause.

The validity of the PBG shall be for a period of 3 years 6 months for Computer Desktops and 5 years 6 months for other equipment.

4. Existing Data Center equipment details :

(i) The server rack (36U) measurements:

Outer width = 23.50 inches
Outer depth = 39.25 inches

Inner width = 20 inches
Inner depth = 28.50 inches

(ii) SAN Switch : Model CISCO MDS 9148
(iii) Core Switch : Model CISCO 4510

In case the quoted solution is not compatible to the existing rack specification mentioned above, the bidders are supposed to include items required to make the solution complete. The items may be racks and all required accessories. The cost of such additional items needs to be included in the Blade enclosure price.

5. TECHNICAL BID:

The Technical Bid shall consists of Annexure-I and Annexure-II

Annexure-I consists of the Eligibility Criteria – Checklist.

Annexure- II consists of the technical specifications of each items ((relevant documents of specifications of items in the bid to be enclosed).

6. FINANCIAL BID:

The Financial Bid consists of the Annexure-III which is the Bill of Quantity (BoQ).

7. Payment Terms:

S. No	Payment Schedule For Hardware	Fee Payable
1.	After delivery, installation/training, commissioning and integration/testing of equipment at the SDC	80% of the contract value
2.	On completion of 6 months on successful completion of commissioning and integration/testing of equipment at the SDC	20% of the contract value

S. No	Payment Schedule For Windows License	Fee Payable
1	After delivery, successful installation/training	100% of the contract value

8. OTHER TERMS AND CONDITIONS:

i. Bidder must give proper compliance statement for the items quoted along with the Make and Model number of the items quoted.

ii. All Taxes should be indicated clearly in the bid document.

iii. Warranty should be as specified in the Annexure-I.

iv. Rates should be Free On Road (FOR) Shillong and should be indicated clearly in the bid document.

v. Rates should be valid for one year from the date of finalization of the Tender.

vi. Items should be delivered within 4 weeks from the date of issue of the Purchase Order.

vii. In case the Tenderers furnish false information their tenders will be rejected and their EMD stands forfeited.

viii. Power of attorney / authority letter in favour of the official signing the tender should be attached.

ix. Selected tenderers should supply as per quoted price failing which the firm would be dis-qualified.

x. MITS reserves the right to make any changes in the terms and conditions of the tender and also reject any or all the bids without assigning any reason thereof.

xi. The tenderers should have back-to-back arrangement with OEM for Warranty and AMC, scanned Certificate for the same should be uploaded along with Technical bid. A Letter for warranty and support from original equipment manufacturer (OEM) shall also be submitted in addition to Manufacturer's Authorization Form. The letter to contain a

confirmation that the bidder shall be availing back to back warranty support from the OEM during the period of warranty for the equipment quoted in the bid.

xii. The Average Annual Turnover of the firm should be at least **₹.2,00,00,000/- (Rupees Two Crores only)** per annum for the last 3 (three) financial years. A certificate from an Auditor/CA needs to be attached as proof.

xiii. The Bidder's Account should not have been declared as a Non- Performing Asset (NPA) in the Books of any bank or financial institution, a certificate to this effect should be obtained from the Auditor who has signed the Balance Sheet of the Bidder as on 31-03-2019 and submitted along with the Bid .

xiv. The bidders should have a functional service center in Shillong/Guwahati with service engineers along with the contact details of the service centers. The Service Engineers should be ready to attend the call within 12 hours of receipt of complaint and any replacement needed for any computer items should be within 15 days.

xv. MITS reserves the right to cancel the order in the event of unsatisfactory services provided.

xvi. Tenderer should ensure that the Spares for the product offered are available for at least 5 years from the date of installation of equipment. No obsolete/end of sale equipment should be supplied.

9. STANDARDS: The Goods supplied under this tender shall conform to the standards mentioned in the Technical Specifications, and, when no applicable standard is mentioned, the authoritative standards appropriate to the Goods' country of origin shall be applicable. Such standards shall be the latest issued by the authority concerned, failing which the supplier would be blacklisted and no further orders shall be issued.

10. PATENT RIGHTS: In the event of any claim asserted by a third party of infringement of copyright, patent, trademark, industrial design rights, etc., arising from the use of the Goods or any part thereof in India, the Tenderer shall act expeditiously to extinguish such claim. If the Tenderer fails to comply and MITS is required to pay compensation to a third party resulting from such infringement, the Tenderer shall be responsible for the compensation to claimant including all expenses, court costs and lawyer fees. MITS will give notice to the Tenderer of such claim, if it is made, without delay. The Tenderer shall indemnify MITS against all third party claims.

11. INSTRUCTIONS TO BIDDERS:

(i) The tender shall comprise of two sections:
   a. Technical bid (Annexure I and II)
   b. Financial bid (Annexure III-BoQ)

(ii) If the tenderer meet all the criteria set for technical bids mentioned above, their financial bids (BoQ) will be opened.

(iii) Digital signature: Bidder should have valid digital signature

(iv) Bid Submission End Date**: 5.00 PM on 6th July, 2020**

(v) Technical Bid Opening through Video Conferencing**: 3.00 PM on 7th July, 2020**

Sd/-
(K. L. Nongbri)
Joint Secretary to the Govt. of Meghalaya
Information Technology & Communications Department
&
Member Secretary, Meghalaya IT Society

ANNEXURE- I: ELIGIBILITY CRITERIA - CHECKLIST

Sl. No	Particulars	Reference of enclosed proof
1	Non Refundable Tender Fee of Rs.1000/-	
2	Earnest Money Deposit of Rs.50,000/-	
3	Attested copy of valid and current District Council's Trading License (TL) for non-tribal tenderers. (For those who do not have the Trading License, they should apply from the office of Autonomous District Councils. Supply order will be issued, if they are declared successful bidder, on production of the TL within one month's time)	
4	Attested copy of MAF Certificate from the Principal Company or OEMs	
5	Attested copy of PAN Number must be enclosed.	
6	Attested copy of upto date Income Tax Clearance Certificate must be enclosed	
7	Attested copy of GST Certificate/Registration must be enclosed	
8	Attested copy of valid and current Professional Tax Certificate	
9	Attested copy of the Experience and Past Performance document on similar work	
10	Affidavit that they have not been blacklisted for the last 3 years.	
11	Warranty: i. 5 years for item no.1 & 2 of Annexure-II ii. 3 years for item no. 5 of Annexure-II	
12	The Average Annual Turnover of the firm should be at least ₹**.2,00,00,000/-** (Rupees two crores**)** for each of the preceding three years.	
13	Service Centre details (Address & Contact Details) along with name & numbers of service engineer	
14	Certificate from Auditor that the Bidder's Account is not declared as NPA	
15	Power of attorney / authority letter in favour of the official signing the tender	

Sd/-
(K. L. Nongbri)
Member Secretary
Meghalaya IT Society

Annexure-II

Technical specifications of items to be procured for MEGHALAYA SDC (MSDC)

Sl. No	Item	Qty	Make	Model	Compliance of Specifications Yes/No/Higher	Remarks
1	Blade Enclosure and Server					
1.01	Blade Enclosure	1 No				*Refer configuration A*
1.02	Blade Server	4 Nos				*Refer configuration B*
2	Unified Threat Management (UTM) / Next generation Firewall (NGFW) with UTM capabilities	2 No				*Refer configuration C*
3	Windows Server OS Latest Version with CALs – Data Center Edition – 8 cores. CALs License for connecting 5 users.	2 Nos				
4	Windows Server OS Latest Version with CALs – Standard Edition – 8 cores. CALs License for connecting 5 users.	2 Nos				
5	Desktops Core i7	9 Nos				*Refer configuration D*

Note: (i) *Quantity mentioned above may varies.*

(ii) For item at sl. 1 (1.01 & 1.02) above, the bidder should ensure that the items are compatible to each other (same OEM) and the rate will be the total of 1.01 & 1.02.

A. Blade Enclosure Specification (minimum specs)

Item	Description of Requirement
Blade Chassis	Solution to house the required number of blade servers in smallest number of enclosures. Industry standard suitable for housing in Standard Server Racks The blade enclosure should offer at least 50% more higher server density per square-foot when compared to the dense 1U Rack servers. Should support a **minimum of 8** nos of Blade servers occupying a max of 12U rack height
	Same enclosure should support Intel Xeon **as well as storage based blades servers.**
	Should support Hot Pluggable & Redundant Management Modules with on board KVM functionality.
	Should provide a highly reliable and high performance mid-plane/back-plane design in the blade enclosure. Should provide detailed technical information.
	Should be able to accommodate the blade servers of specifications mentioned in the proposed blade enclosures. The proposals must offer the most dense packaging possible for the blade servers in the enclosure and maximum headroom for future expansion in the offered enclosures.
	Support simultaneous remote access for different servers in the enclosure.
Interconnect	Should support simultaneous housing of FCoE, Ethernet, FC and SAS interconnect fabrics offering Hot Pluggable & Redundancy as a feature
Blade Server Interconnect to LAN/ Network	The uplink from the chassis should support redundant links for both ethernet and FC. The enclosure should support network switches with at least 2 Nos of 1 GB uplink ports, up-linkable to the data center switch. The port in the existing switch of MSDC - CISCO 4510 is 1 GB port and bidders are supposed to provide a solution compatible to connect to an existing equipment to make the solution complete.
Blade Server Interconnect to Fiber Channel SAN	The enclosure should support Fiber Channel SAN switches with at least 8 Gb auto-negotiating FC uplinks and also at least 8Gb auto-negotiating downlinks to all server bays. Bidder are supposed to provide a solution compatible to connect to an existing SAN switch at MSDC - model CISCO MDS 9148 to make the solution complete.
Power Supply	The enclosure should be populated fully with power supplies of the highest capacity available with the vendor. Power supplies should support N+N as well as N+1 redundancy configuration, where N is greater than 1. Should offer a single phase power subsystem enabled with technologies for lower power consumption and offering high energy efficiency levels. Vendors should provide documents certifying the claims.
Cooling	Each blade enclosure should have a cooling subsystem consisting of redundant hot pluggable fans or blowers enabled with technologies for improved power consumption and acoustics.
Warranty	5 years comprehensive warranty.
System Software	Management/controlling software have to be from the OEM.

Remote Management	Must provide a remote management functionality to operate the server in both in-band and out-of-band. Must be part of the server without the need to install any additional hardware or software.
	Must have a real time Virtual KVM functionality and be able to perform a remote Power sequence. Must provide both Java & Java-free browsing options.
	Must have the ability to map the remote media to the server and ability to transfer files from the user's desktop/laptop folders to the remote server with only the network connectivity.
	Must have the ability to capture the video sequence of the last failure and the boot sequence and also playback the video capture or equivalent technology.
	Must have the ability for multiple administrators across remote locations to collaborate on the remote session in a server with multiple sessions even in server powered OFF mode.
Power Management	Must be able to show the actual power usage and actual thermal measurement data of the servers.
Compliance	Vendors must submit supporting documents stating RoHS compliance.

Note : In case the quoted solution is not compatible to the existing rack specification mentioned in the Tender, the bidders are supposed to include items required to make the solution complete. The items may be racks and all other required accessories. The cost of such additional items needs to be included in the Blade enclosure price.

B. Blade Server Specification: (minimum specs)

Item	Description of Requirement
CPU	At least Two Nos. Latest generation Intel® Xeon with 8-cores or above processors. Free PCIe slots for expansion, clock speed > 2.5GHz
CPU L3 CACHE Memory	8.25 MB L3 or above cache depending upon processor model chosen
Motherboard	Intel® C621 Series Chipset or above.
Memory	Server should have minimum 64GB of DDR3/DDR4 memory Should have at least 24 DIMM slots per blade, supported up to 1.5 TB of DDR3/DDR4 memory.
Memory Protection	Advanced ECC with multi-bit error protection.
Storage	2 * 300 GB or above hot plug SFF SAS/SSD/SATA drives.
Storage Controller	Server should have 12Gb/s SAS Raid Controller with RAID 0/1/1+0 with 1GB Flash Backed Write Cache.
Networking features	One of below embedded ports should be provided: 1. Dual Port 20GbE Converged Network Adaptor which supports partitioning up to 7* Ethernet and 1* FC/iSCSI HBA ports per 20Gbps port 2. Dual port 10GbE Converged Network Adaptor which supports partitioning up to 3* Ethernet and 1* FC/iSCSI HBA ports per 10Gbps port
Interfaces	Minimum of 1 * internal USB 3.0 port .

Blade Server Connectivity to SAN	Should be provided with 1 No 16 Gbps Dual port Fiber Channel HBA internal to the Server Blade.
Bus Slots	Minimum of 2Nos of 3.0 PCIe x16 based mezzanine slots supporting Converged Ethernet, Ethernet, FC adapters and SAS adaptors
Industry Standard Compliance	ACPI 6.1 Compliant PCIe 3.0 Compliant WOL Support Microsoft® Logo certifications PXE Support USB 3.0 Compliant SMBIOS 3.1 UEFI 2.6 Redfish API
Embedded system management	Should support monitoring ongoing management, service alerting, reporting and remote management with embedded Gigabit out of band management port. Server should support configuring and booting securely with industry standard Unified Extensible Firmware. System should support RESTful API integration. System management should support provisioning servers by discovering and deploying 1 to few servers with Intelligent Provisioning. System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support
Security	UEFI Secure Boot and Secure Start support. Security feature to ensure servers do not execute compromised firmware code. Support for Commercial National Security Algorithms (CNSA) Granular control over remote management interfaces or equivalent industry methods. Tamper-free updates - components digitally signed and verified Secure Recovery - recover critical firmware to known good state on detection of compromised firmware TPM (Trusted Platform Module) 1.2 option TPM (Trusted Platform Module) 2.0 option Bezel Locking Kit
OS Support	Microsoft Windows Server VMware Red Hat Enterprise Linux Server SUSE Linux Enterprise Server
Secure encryption	System should support Encryption of the data on both the internal storage and cache module of the array controllers using encryption keys. Should support local key management for single server and remote key management for central management for enterprise-wide data encryption deployment.
Warranty	5 year comprehensive warranty
Provisioning	Essential tools, drivers, agents to setup, deploy and maintain (not the OS) the server should be embedded inside the server. There should be a built - in update manager that can update these tools online.
Firmware security	1. For firmware security, system should support remote management chip creating a fingerprint in the silicon, preventing servers from booting up unless the firmware matches the fingerprint. This feature should be immutable

	2. Should maintain repository for firmware and drivers recipes to aid rollback or patching of compromised firmware. Should also store Factory Recovery recipe preloaded to rollback to factory tested secured firmware
Embedded Remote Management and firmware security	1. System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder; It should support server power capping and historical reporting and should have support for multifactor authentication 2. Server should have dedicated remote management port 3. Remote management port should have storage space earmarked to be used as a repository for firmware, drivers and software components. The components can be organized in to install sets and can be used to rollback/patch faulty firmware 3. Server should support agentless management using the out-of-band remote management port 4. The server should support monitoring and recording changes in the server hardware and system configuration. It assists in diagnosing problems and delivering rapid resolution when system failures occur 5. Applications to access the server remotely using popular handheld devices based on Android or Apple IOS should be available 6. Remote console sharing upto 2 users simultaneously during pre-OS and OS runtime operation, Console replay - Console Replay captures and stores for replay the console video during a server's last major fault or boot sequence. Microsoft Terminal Services Integration, 128 bit SSL encryption and Secure Shell Version 2 support. Should provide support for AES and 3DES on browser. Should provide remote firmware update functionality. Should provide support for Java free graphical remote console. 7. Should support managing multiple servers as one via Group Power Control Group Power Capping Group Firmware Update Group Configuration Group Virtual Media Group License Activation 8. Should support RESTful API integration 9. System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support
Server Management	Software should support dashboard view to quickly scan the managed resources to assess the overall health of the data center. It should provide an at-a-glance visual health summary of the resources user is authorized to view.
	The Dashboard minimum should display a health summary of the following: • Server Profiles • Server Hardware • Enclosures • Logical Interconnects • Appliance alerts
	The Systems Management software should provide Role-based security

	Software should support search for resource-specific information such as specific instances of resource names, serial numbers, WWNs, IP and MAC addresses to help manage infrastructure better
	Management software should support integration with popular virtualization platform management software like vCenter, SCVMM and RedHat RHEV
	Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD.
	Should provide an online portal that can be accessible from anywhere. The portal should provide one stop, online access to the product, support information and provide information to track warranties, support contracts and status. The Portal should also provide a Personalised dashboard to monitor device heath, hardware events, contract and warranty status. Should provide a visual status of individual devices and device groups. The Portal should be available on premise (at our location - console based) or off premise (in the cloud).
	Should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components.
	The Server Management Software should be of the same brand as of the server supplier.

C. Unified Threat management (UTM) / Next generation Firewall (NGFW) with UTM capabilities (minimum specs)

General Requirements	
1	Network security appliance should support "Stateful" policy inspection technology. It should also have application intelligence for commonly used TCP/IP protocols like telnet, ftp, SSH etc.
2	The proposed vendor must have a track record of continuous improvement in threat detection (IPS) and must have successfully completed NSS Labs' NGFW Methodology latest version testing with a minimum exploit blocking rate of 98% or should be available on Gartner report for firewalls.
3	Proposed vendor must be in Leader quadrant of Gartner Magic Quadrant for Enterprise Firewall as per the latest report
4	Proposed vendor must be in Leader quadrant of Gartner Magic Quadrant for Enterprise Firewall as per the latest report
5	Configuration Support for the firewall.
6	Configuration training
7	Security patches /IOS/ UTM S/W etc updates for the solution be available for a period of minimum 5 years. 24x7 Comprehensive Support, Advanced Hardware Replacement (NBD), Firmware and General Upgrades
Hardware & Interface requirements	

1	The platform must be supplied with minimum **2x 10GE SFP**+/GE SFP, 4x GE SFP, 8 x GE RJ45 interface Slots
2	The Appliance should have dedicated Console , 1 Management and 1 USB ports.
3	The Appliance should support out of band management.
Performance and Availability	
1	Solution should provide minimum Firewall throughput of 20 Gbps
2	10,00,000 minimum concurrent sessions.
3	Minimum IPS throughput of 4 Gbps on real world.
4	Minimum Threat prevention throughput (measured with Firewall, Application Control, IPS & Anti-Malware enabled on real world or enterprise traffic mix) of 4 Gbps
5	Minimum NGFW 5 Gbps
6	IPSec VPN throughput: minimum 5 Gbps
7	100 SSL VPN User support
8	The solution should support minimum 5 virtual firewalls **/virtual route tables**
9	Internal Storage should be minimum 100 GB
Routing Protocols	
1	Static Routing
2	Policy Based Routing
3	The Firewall should support Dynamic Routing Protocol for RIP1 & 2, OSPF, OSPFv3, BGPv4/ BGPv6, RIPng
ZERO DAY Protection	
1	Firewall should Support Zero day attack
Firewall Features	
1	Firewall should provide application inspection for LDAP, SIP, H.323, SNMP, FTP,SMTP, HTTP, DNS, ICMP, DHCP, RPC, IMAP, NFS etc
2	IPv6-enabled inspection services for applications based on HTTP, FTP, SMTP, ICMP, TCP and UDP
3	Allows secure deployment of next-generation IPv6 networks, as well as hybrid environments that require simultaneous, dual stack support of IPv4 and IPv6

4	The firewall should support transparent (Layer 2) firewall or routed (Layer 3) firewall Operation
5	The Firewall should support ISP link load balancing.
6	Firewall should support link aggregation functionality to group multiple ports as single port.
7	Firewall should support minimum VLANS 1024
8	Firewall should support static NAT, policy based NAT and PAT
9	Firewall should support IPSec data encryption
10	It should support the IPSec VPN for both site-site and remote access VPN
11	Firewall should support IPSec NAT traversal.
12	Support for standard access lists and extended access lists to provide supervision and control
13	control SNMP access through the use of SNMP and MD5 authentication.
14	Firewall system should support virtual tunnel interfaces to provision route-based IPSec VPN
15	The Firewall should have integrated solution for SSL VPN
16	It should support the authentication protocols RADIUS, LDAP, TACACS, and PKI methods
17	Licensing should be a per device and not user or IP based
Integrated IPS Features Set	
1	IPS should able to detect malicious traffic in IPV4, IPV6 and hybrid IPV6 and IPV4 network environment
2	IPS should have DDoS and DoS anomaly detection and protection mechanism with automatic threshold configuration.
3	Signature based detection using real time updated database & should have minimum 10000+ IPS signature database from day one
4	Support SYN detection and protection for both targets and IPS devices.
5	The device shall allow administrators to create Custom IPS signatures
6	Should have a built-in Signature and Anomaly based IPS engine on the same unit
7	Signature based detection using real time updated database
8	Supports automatic security updates directly over the internet. (ie no dependency of any intermediate device)
9	Security check updates do not require reboot of the unit.

10	Configurable IPS filters to selectively implement signatures based on severity, target (client/server), protocol, OS and Application types.
AntiVirus & AntiBot	
1	Firewall should support antimalware capabilities, including antivirus and botnet traffic filter.
2	Solution should be able to detect and prevent unique communication patterns used by BOTs i.e. information about botnet family
4	Solution should be able to block traffic between infected host and remote operator and not to legitimate destination
5	Solution should be able to provide protection from mobile malwares
6	Solution should have an option of packet capture for further analysis of the incident
7	Solution should uncover threats hidden in SSL links and communications
8	The AV/**Antimalware** should scan files that are passing on CIFS protocol
10	The proposed system shall provide ability to allow, block attachments or downloads according to file extensions and/or file types
11	The proposed system should be able to block or allow oversize file based on configurable thresholds for each protocol types and per firewall policy.
12	The proposed silution should be able to detect unknown malware or zero day threats by integrating with a cloud based sandboxing solution
Other support	
1	Should support features like Web- Filtering, Application-Control from day one.
2	The proposed system should have integrated Enterprise-class Web Content Filtering solution with database which should support over 450 million webpages in 72+ categories and 68+ languages without external solution, devices or hardware modules.
3	Should support detection over 3,000+ applications in multiple Categories: Botnet, Collaboration, Email, File Sharing, Game, General Interest, Network Service, P2P, Proxy, Remote Access, Social Media, Storage Backup, Update, Video/Audio, VoIP, Industrial, Special, Web (Others)
4	QoS features like traffic prioritization, differentiated services,. Should support for QoS features for defining the QoS policies.
5	It should support the VOIP traffic filtering
6	Appliance should have identity awareness capabilities
7	The firewall must work as an Active-Active or Active-Standby redundancy with 2 hardware UTM box
8	Solution must support VRRP clustering protocol or equivalent

Management & Reporting functionality	
1	Support for Built-in Management Software for simple, secure remote management of the security appliances through integrated, Web-based GUI.
2	Support accessible through variety of methods, including console port, Telnet, and SSHv2
3	Support for both SNMPv2 and SNMPv2c, providing in-depth visibility into the status of appliances.
4	The solution should have option for firewall configuration audit & compliance check to be done in automated or manual process
5	Extensive Logging, reporting for all the UTM functionalities offered should be available. A minimum usable storage capability of 800 GB need to be provided with the solution. It should support log analysis from day one.
6	The offered solution should support creation of customized reports
7	Should have reporting functionality base on Applications, Users, Threats, Traffic etc.
8	Should capable to provide a convenient method for alerting administrators when critical events are encountered, by sending e-mail alert messages to administrator defined e-mail addresses
9	Solution must allow administrator to choose to login in read only or read-write mode
10	5 years 24x 7 support is required
11	In case of hardware failure, Next day delivery should be available.
12	Operating Temperature Range (Degree C) - **0-40**
13	Operating Humidity (RH) (%)- 10 to 90

D. Desktop Core i7 or equivalent

1. CPU: Intel Core i7 (9th Generation and above) or equivalent
2. Memory: 8 GB DDR4 RAM with 32 GB Expandability.
3. Hard Disk Drive: 256GB M.2 SATA SSD (Boot) + 1TB SATA
4. Monitor: 21.5" Full HD LED Display,
   Resolution: 1920 x 1080 Pixel
5. Input Devices: Wireless Mouse and Wireless Keyboard
6. Warranty: Comprehensive 3 Years
   Warranty
7. Motherboard OEM Motherboard with logo embossed (no sticker)
8. Industry Standard & Certification:
   FCC Compliance, EPEAT Certification or equivalent
9. Minimum 4 USB Ports (at least 1 USB 3.1) out of which 2 USB ports should be in front for easy access, (1) HDMI Port, (1) RJ-45 network connector, 1 universal audio jack for earphone & MIC, 1 audio line in, 1 audio line out.

Sd/-
(K. L. Nongbri)
Joint Secretary to the Govt. of Meghalaya
Information Technology & Communications Department
&
Member Secretary
Meghalaya IT Society