

TENDER

FOR

SUPPLY, INSTALLATION AND COMMISSIONING

OF

BROADBAND INTERNET FACILITY WITH WI-FI

AT

BOY'S HOSTELS

OF

INDIRA GANDHI INSTITUTE OF MEDICAL SCIENCES, PATNA



Tender No.: 02 / WI-FI HOSTEL / BME / 2020

Last Date of submission: 21.09.2020 up to 4 P.M.



INDIRA GANDHI INSTITUTE OF MEDICAL SCIENCES,

SHEIKHPURA, PATNA – 800 014 (Bihar, India)

Tel.: 0612 – 2297631, 2297099; Fax: 0612 – 2297225; Website: www.igims.org;

E-Mail: director@igims.org / bme@igims.org

Page 1 of 25

Background:

Indira Gandhi Institute of Medical Sciences, Sheikhpura, Patna - 800 014 is the premiere medical institute of the state of Bihar - established by the act of Assembly and functioning under Department of Health, Government of Bihar. Various facilities are being developed at this Institute to cater to needs of patients belonging to the state of Bihar and neighbouring states.

Indira Gandhi Institute of Medical Sciences, Patna is a tertiary care hospital, providing treatment in various super-specialties and broad specialities. Patients are often referred from various hospitals and medical colleges. Patients come here with high hopes for highly specialised treatment and care. The institute is also running **Medical College with an annual intake of 120 students apart from various P.G. and Diploma courses for doctors and paramedical staffs.**

Institute intent to provide Broadband Internet facility with Wi-Fi at new and old Boy's Hostels for use by UG / PG students

Indira Gandhi Institute of Medical Sciences, Patna (IGIMS) invites tender for supply, erection, installation, commissioning, testing, demonstration and maintenance of Broadband Internet facility with WI-FI at Boy's Hostels, as per specifications given in the Annexure attached to the Tender form. All offers should be made in English and should be written in both figures and words. Tender forms can be downloaded from the Institute website (<http://www.igims.org>) of the Institute.

The bidders are requested to read the tender document carefully and ensure compliance with all specifications/instructions herein. Non-compliance with specifications/instructions in this document may disqualify the bidders from the tender exercise. The Director, Indira Gandhi Institute of Medical Sciences, Patna reserves the right to select the item (in single or multiple units) or to reject any quotation wholly or partly without assigning any reason. Incomplete tenders, amendments and additions to tender after opening or late tenders are liable to be ignored and rejected.

Terms and Conditions:

1. The technical and financial bids should be quoted separately and put in different sealed envelopes marked "**Technical bid**" or "**Financial bid**" as applicable. These separate bids envelopes are to be put in an outer envelope which should also be sealed.
2. The Vendors who have earlier supplied the equipment to reputed Govt. / Pvt. Institutions / Organizations and other Medical / Scientific Institute of National / State Repute may only tender. The details of such institutions and the cost with name of equipment may also be supplied with the bids.
3. The technical and financial bids should be submitted in original. The financial bid should include the cost of main equipment/item and its accessories. If there is any separate cost for installation etc. that should be quoted separately.
4. Each individual sealed envelope as well as the outer envelope should be marked with the following reference on the top left hand corner: "**Tender Notice No.: 02 / WI-FI HOSTEL / BME / 2020; Item Name: Supply, Installation and Commissioning of Broadband Internet Facility with Wi-Fi**".

5. The printed literature and catalogue/brochure giving full technical details should be included with the technical bid to verify the specifications quoted in the tender. The bidders should submit copies of suitable documents in support of their reputation, credentials and past performance.
6. The rates should be quoted in figures (typed or printed) and cutting should be avoided. The final amount should be in figures as well as in words. If there are cuttings, they should be duly initialed, failing which the bids are liable to be rejected.
7. Any bids received after 4:00 P.M. on 21.09.2020 shall not be considered
8. The Technical Bids will be opened on 22.09.2020 at 03:00 P.M. The date & time for opening of Financial Bids will be informed later on to the technically qualified bidders.
9. While sending rates, the firm shall give an undertaking to the effect that *“the terms/conditions mentioned in the enquiry letter/Tender Notice against which the rates are being given are acceptable to the firm.”* In case the firms do not give this undertaking, their rates will not be considered.
10. If the supplier/firm is original equipment manufacturer (OEM)/authorized dealer/sole distributor of any item, the certificate to this effect should be attached.
11. The quantity shown against the item is approximate and may vary (increase or decrease) as per demand of the Institute at the time of placing order.
12. All tender documents should have to be sent through courier, speed post or registered post only. All tender documents received after the specified date and time shall not be considered.

The postal address for submitting the tenders is:

**The Director,
Indira Gandhi Institute of Medical Sciences,
Sheikhpura,
Patna – 800 014 (Bihar)**

13. In the event of any dispute or difference(s) between the vendee Institute (IGIMS, Patna) and the vendor(s) arising out of non-supply of material or supplies not found according to specifications or any other cause whatsoever relating to the supply or purchase order before or after the supply has been executed, shall be referred to “The Director, IGIMS, Patna”, who may decide the matter himself or may appoint arbitrator(s) under the arbitration and conciliation Act,1996. The decision of the arbitrator shall be final and binding on both the parties.
14. The place of arbitration and the language to be used in arbitral proceedings shall be decided by the arbitrator.
15. All disputes shall be subject to Patna (Bihar) Jurisdiction only.
16. All tenders in which any of the prescribed conditions is not fulfilled or any condition is put forth by the tenderer shall be summarily rejected.
17. IGIMS, Patna reserves the right to cancel the tender at any point of time without assigning any reason.

18. The bidders or their authorized representatives may also be present during the opening of the Technical Bid, if they desire so, at their own expenses.

Note: Price bids of only those bidders will be opened whose technical bids are found suitable by the committee appointed for the purpose. Date and time of opening of price bids will be decided after technical bids have been evaluated by the committee. Information in this regard will be intimated to the technically qualified bidders. In exceptional situation, an authorized committee may negotiate price with the qualified bidder quoting the lowest price before awarding the contract.

19. **Clarifications:**

In case the bidders requires any clarification regarding the tender documents and technical specifications, they are requested to contact our office through e-mail (e-mail: bme@igims.org) on or before 29 /08 / 2020.

20. **Tender Cost:**

A Demand draft of **Rs. 2,000/- (Rupees Two Thousand only)** towards non-refundable tender fee, drawn in favour of “**The Director, IGIMS, Patna**” payable at **Patna (Bihar)** should accompany the Technical bid documents. In the absence of tender cost, the tender will not be accepted.

21. **Earnest Money Deposit (EMD):**

A refundable amount of **Rs. 50,000/- (Rs. Fifty Thousand Only)** as earnest money deposit (EMD) in the shape of DD from a scheduled bank in India (valid for a minimum period of 3 months from the date of submission of tender) should accompany the bid documents. The DD drawn in favour of “The Director, IGIMS, Patna” payable at Patna (Bihar) should accompany the bid documents. The EMD should be kept in a separate sealed envelope, should be marked clearly and put in the outer envelope that contains the technical and financial bid envelopes. The bidders should enclose a pre-receipted bill for the EMD to enable us to return the EMD of unsuccessful bidders. Failure to deposit Earnest Money will lead to rejection of tender. The bidders should submit separate EMD. In the event of the awardees bidder backing out, EMD of that bidder will be forfeited.

22. **Pre – Qualification Criteria:**

- a. Bidders should be the manufacturer / authorized dealer. Letter of Authorization from original equipment manufacturer (OEM) on the same and specific to the tender should be enclosed.
- b. The Vendors who have earlier supplied the equipment to reputed Govt. / Pvt. Institutions / Organizations and other Medical / Scientific Institute of National / State Repute may only tender. The details of such institutions and the cost with name of equipment may also be supplied with the bids.
- c. An undertaking from the OEM is required stating that they would facilitate the bidder on a regular basis with technology/product updates and extend support for the warranty as well.
- d. OEM should be internationally reputed Branded Company.
- e. Non-compliance of tender terms, non-submission of required documents, lack of clarity of the specifications, contradiction between bidder specification and supporting documents etc. may lead to rejection of the bid.

- f. Furnishing of wrong/ambiguous information in the compliance statement may lead to rejection of bid and further black listing of the bidder, if prima-facie it appears that the information in the compliance statement was given with a malafide/fraudulent intent.

23. Prices:

- a. The Prices quoted should be inclusive of all taxes or duties, packing, forwarding, freight, insurance, delivery and commissioning etc. at destination site (IGIMS, Patna). The rates shall be firm and final. Nothing extra shall be paid on any account. In the price bid/financial bid, the vendor should clearly mention the final price breakup i.e. Ex-work price/FCA price, FOB price, CIP/CIF price & FOR IGIMS, Patna Campus price, as applicable in their bid.
- b. In case of imported equipment(s)/item(s), the agency commission, if any, payable in Indian rupees should be mentioned separately. For imported equipment, the Letter of Credit will be opened for the amount excluding agency commission in Indian Rupees. The firm should clearly mention the address of foreign bank in the financial bid.

24. Validity:

The bid should be valid for acceptance up to a period of 180 Days. The Bidders should be ready to extend the validity, if required without any additional financial implications.

25. Delivery:

The Equipment should be delivered and installed within the period as specified in the purchase order and be ready for use within 4 weeks of the issue of purchase order unless otherwise prescribed. If the bidder fails to deliver and place any or all the Equipments or perform the service by the specified date, penalty at the rate of 2% per week of the total order value subject to the maximum of 10% of total order value will be deducted.

26. Training:

Bidders need to provide adequate training to the nominated persons of IGIMS, Patna at their cost. IGIMS, Patna will not bear any training expenditure.

27. Warranty Declaration:

Bidders must give the comprehensive on-site warranty as required from the date of successful installation of Equipment against any manufacturing defects and also give the warranty declaration that *“everything to be supplied by us hereunder shall be free from all defects and faults in material, workmanship and shall be of the highest quality and material of the type ordered, shall be in full conformity with the specification and shall be complete enough to carry out the experiments, as specified in the tender document.*

Any deviation in the material, and the specifications from the accepted terms may liable to be rejected and the bidders need to supply all the goods in the specified form to the satisfaction / specifications specified in the order / contract and demonstrate at their own cost.

- 28. Warranty / Guarantee / CAMC:** The successful bidder should provide **comprehensive warranty for three years for all components without any additional cost to the purchaser form the date of satisfactory commissioning.** Components include all parts (accessories / consumables / spares parts) of SCS. All accessories/ consumable / spare parts replaced shall be from OEM / Supplier of same model or higher version. If within a

period of three years after commission, any accessory / consumable/ spare part is proved to be defective then such product shall be replaced by the manufacturer / supplier. Such replacement shall be sole obligation of manufacturer / supplier, including payment of charges for freight delivery, custom duty and transportation, if any.

29. In case of breakdown during the warranty period, a competent Service Engineering of the supplier should make as many visits as are required to rectify the problem and replace the faulty parts, without any liability of cost. Service response time must be less than 72 hours. Bidder is also required to quote rate for Comprehensive Annual Maintenance Contract including all parts (spares and consumables) for a further period of two after expiry of warranty period of three years. It is essential to quote CAMC failing which the bid will not be evaluated and summarily rejected.
30. During warranty period and as well as during Comprehensive Annual Maintenance Contract period, successful bidder will maintain the network with a **uptime of 95% of 365 days (i.e. Uptime = 347 days per year)** . Any uptime below 347 days will be compensated by the successful bidder by increasing the period of warranty / Comprehensive Annual Maintenance Contract period by one day equal to one week.
31. Successful bidder is required to submit **certificate** to the effect that the price quoted by them is the lowest price and they have not supplied the required items at the price lower than the quoted price to any other Govt. Hospital / Nursing Home / Institution / organization.
32. **Terms of Payment:** 90% Payment will be made only after delivery and satisfactory installation, testing, commissioning etc. and on submission of satisfactory working report issued by the officials as authorized by the Institute. The remaining 10% will be released after expiry of warranty period or on submission of Bank Guarantee of the same value with a validity to cover warranty period.
33. **Tender expenses and documents:** All costs incurred by the bidder in the preparation of the tender shall be at the entire expense of the bidder.
34. **Tender Evaluation Criteria:** The technical bids will be opened and evaluated by a duly constituted committee. After evaluation of the technical bid, the financial bid for only those offers which have qualified in the evaluation of technical bid will be opened.
35. **Return of EMD:**
 - The earnest money of unsuccessful bidders will be returned to them without any interest within 15 working days after awarding the contract.
 - The earnest money of the successful bidder will be returned to them without any interest within 15 Days after supply of material.
36. **Manual and documentation:** All the manuals necessary for operating and servicing the equipment (including details of electronic circuits) will have to be provided along with the instrument.
37. The IGIMS, Patna reserves the right to cancel the tender at any stage (point of time) without assigning any reason.
38. Bidders should go through the tender terms, conditions and specifications carefully and fill in the attached compliance statement accurately and unambiguously. They should ensure that all the required documents are furnished along with the bid.



**Director,
I.G.I.M.S. – Patna.**

BID PARTICULARS

1. Name of the Supplier :

2. Address of the Supplier :

3. Availability of demonstration of equipment : Yes / No

4. Tender cost enclosed: : Yes/No if yes

D. D. No. _____ Bank _____ Amount _____

5. EMD enclosed : Yes / No if (Yes)

D. D. No. _____ Bank _____

6. Name and address of the Officer/contact person to whom all references shall be Made regarding this tender enquiry.

Name :

Address :

Telephone No.:

Fax No. :

Mobile No :

E-Mail :

Web :

Ref:- Tender Notice No.:

S. No.	Minimum Technical Specifications	Compliance Yes/No
	Make: _____ Model/ Part No. _____	
Item Name	Dual Band Wireless-AC Access Point	
1	Physical Interfaces	
	One (1) 10/100/1000BASE-T Gigabit Ethernet (RJ-45) ports with Auto Uplink™ (Auto MDI-X) with IEEE 802.3af or 802.3at Power over Ethernet (PoE) support	
	One (1) console port with RJ45 Interface	
	Two (2) Internal 5/6dBi (2.4/5GHz)	
	Two (3) reverse SMA antenna connectors for dual band 2.4 and 5GHz external antennas (not included)	
	Five (5) LED: Power, Link/ACT, LAN, 2.4GHz, 5GHz	
	Power adapter (not included): 12V DC, 2.5A	
2	Standards	
	IEEE 802.11ac, IEEE 802.11g, IEEE 802.11b, IEEE 802.11n	
	IEEE 802.11ac Wave1 standard, 2.4GHz and 5GHz	
	WMM - Wireless Multimedia Prioritization	
	WDS- Wireless Distribution System	
	Power over Ethernet (PoE) IEEE 802.3af/802.3at	
3	Security	
	Wi-Fi Protected Access (WPA, WPA2), 802.11i	
	Wired Equivalent Privacy (WEP) 64-bit, 128-bit, and 152-bit encryption	
	IEEE 802.1x RADIUS authentication with EAP TLS, TTLS, PEAP	
	Wireless access control to identify authorized wireless network devices	
	MAC address filtering with access control	
	Multiple VPN pass-through support	
	Secure SSH Telnet	
	Security Socket Layer (SSL) remote management login	
	Remote management login	
	MBSSID/VLAN Support 16/17	
	Peer-to-peer blocking so users may not access another user's PC	
4	Network Management	
	Ensemble Management for support of up to 10 like Access Points in a single cluster	
	Remote configuration and management through Web browser, SNMP or Telnet with command line interface (CLI)	
	SNMP management supports SNMP MIB I, MIB II, 802.11 MIB and proprietary configuration MIB	
5	Manageability	
	As standalone	

	Cluster Mode	
	Controller	
6	Advanced Wireless Features	
	Wireless Distribution System (WDS)	
	Bridge mode: Point-to-point wireless WDS mode	
	Bridge mode: Point-to-multipoint wireless WDS mode	
	Repeater mode	
	Adjustable Transmit Power Control (TPC)	
7	Other Specifications	
	PoE power consumption: 12.9W maximum	
	Bonjour Gateway	
	Band steering	
	Link Layer Discovery Protocol	
	Rogue AP detection	
	Block SSID Broadcast	
	MBSSID/VLAN Support: 16/17	
	Ceiling mounting/ Wall mounting	
	3x3 SU-MIMO support	
	an aggregate throughput of up to 1.75 GBps (450 Mbps for 2.4 GHz and 1300 Mbps 802.11ac for 5 GHz)	
	Max number of Concurrent Clients: 128	
	Deployment Options: Standalone, Controller & Ensemble Mode	
	Rate Limiting	
	Approved Make: Cisco /Sophos /Dell/Netgear	
8	Warranty and Support	
	Lifetime free latest firmware support	
	Replacement with New Product Only No refurbished Products.	
S. No.	Minimum Technical Specifications	Compliance Yes/No
Item Name	High Performance Enterprise-Class Wireless Controller with 50 AP Support	
	Physical Specifications	
1	4# 1GBps auto-sensing and auto-negotiation ports for Data and Control	
	1# USB 2.0 port	
	1# DB-9 Console port	
	Rack Mountable	
	LED: Power, status, fan and stacking master	
	Default Reset	
	Software Specifications	
2	Supports up to 50 Access Points and 2,000 concurrent clients per controller	
	Stack up to 3 controller per wireless cluster	
	Supports up to 150 Access Points and 6,000 concurrent clients per controller cluster	

	Ufast AP discovery provides super-fast AP discovery	
	Secured communication between AP and Controller	
	Data traffic can be forwarded to the best path without traversing the controller	
	Eliminates controller bottleneck for high throughput 802.11n & 802.11ac APs	
	Intelligent tunneling with Layer 2 and Layer 3 roaming	
	Layer 2 and Layer 3 seamless roaming	
	WLAN healing for automatic RF coverage in the case of AP failure	
	Rogue AP detection	
	Support both indoor and outdoor APs	
	Support 802.11b, 802.11g, 802.11n, 802.11a and 802.11ac	
	Support access points discovery in the network, even across VLANs and subnets	
	RF Management	
3	Automatic channel distribution to minimize interferences	
	Auto-channel allocation taking into consideration of the environment, interferences, traffic load and neighboring AP	
	Scheduled mode for Auto-channel allocation	
	Automatic mode in case of high level of interferences available	
	Optimum transmit power determination based on coverage requirements	
	Automatic power control mode available	
	Neighborhood scan of RF environment to minimize neighboring AP interference and leakage across floors	
	Automatic mode or Manual mode for Coverage Hole Detection	
	Down APs or compromised RF environment detection with alerts	
	Self healing: automatic neighboring AP power increase to cover coverage losses	
	APs load monitoring and overloading prevention	
	Clients redirection to lightly loaded neighboring APs	
	Seamless rapid mobility across VLAN and subnets	
	Including 802.11i pre-auth and fast roaming	
	Fast Roaming support across L2, and L3 for video, audio and voice over wireless client	
	Bandsteering to optimally load balance traffic between 2.4 and 5GHz	
	QoS	
4	WMM (802.11e) support	
	WMM Queues in decreasing order of priority	
	WMM Power Save option	
	Wireless Security	
5	Open, WEP, WPA/WPA2-PSK	

	802.11i/WPA/WPA2 Enterprise with standard interface to external AAA / RADIUS Server	
	Distinct AAA Server per SSID	
	RADIUS Accounting Protocol	
	LDAP Based Authentication & Microsoft® Active Directory Server	
	Per Client Based LDAP policies for user bandwidth rate limiting available	
	Integrated AAA Server	
	Integrated Captive Portal available for client authentication in a Security Profile	
	Password based authentication mode: local user store available, receptionist assigned user name / password	
	Open authentication mode: guests auto registration with email address (up to 64 email stored)	
	Extraction of logs of guest activity	
	Captive Portal: Configurable Portal page, including image files	
	Detection and Mapping of up to 512 Rogue APs	
	Wireless Network Monitoring	
6	Summary of the Managed Access Points status, rogue Access Points detected, Wireless stations connected, Wireless Controller Information and Wireless Network usage	
	APs status for the Managed Access Points and details that includes configuration settings, current Wireless settings, current Clients and detailed Traffic statistics	
	Rogue Access Points: Reported, in same channel and in interfering channels	
	Wireless Clients statistics and details per AP, per SSID, per floor, per location	
	Black listed Clients, Roaming Clients	
	Wireless Network Usage: show Ethernet, Wireless 802.11 b/bg/ng and 802.11 a/na mode traffic separately	
	DHCP details for Wireless Clients	
	Management	
7	HTTP, SNMP v1/v2c, Telnet, Secure Shell (SSH)	
	Logging and Reporting	
	Managed Access Points Ping	
	Save/Restore Configuration	
	Firmware Upgrade via Web browser for the Wireless Controller and the Managed Access Points	
	Support Dual Boot Image	
	IEEE and RFC Standards	
8	IEEE 802.3 10BASE-T	
	IEEE 802.3u 100BASE-TX	
	IEEE 802.3ab 1000BASE-T	

	IEEE 802.1Q VLAN tagging	
	IEEE 802.11i	
	IEEE 802.1X	
	RFC 2131 DHCP	
	RFC 768 UDP	
	RFC 791 IP	
	RFC 792 ICMP	
	RFC 793 TCP	
	RFC 1519 CIDR	
	RFC 1542 BOOTP	
	WPA-PSK, WPA2-PSK	
	WEP and TKIP-MIC: RC4 40, 104 and 128 bits (both static and shared keys)	
	AES: CBC, CCM, CCMP	
	DES: DES-CBC, 3DES	
	SSL and TLS: RC4 128-bit and RSA 1024- and 2048-bit	
	DTLS: AES-CBC	
	IPSec: DES-CBC, 3DES, AES-CBC	
	RFC 2406 IPsec	
	RFC 2409 IKE	
	RFC 3280 Internet X.509 PKI Certificate and CRL Profile	
	RFC 3602 The AES-CBC Cipher Algorithm and Its Use with IPsec	
	RFC 3686 Using AES Counter Mode with IPsec ESP	
	RFC 4347 Datagram Transport Layer Security	
	RFC 4346 TLS Protocol Version 1.1	
	RFC 2548 Microsoft Vendor-Specific RADIUS Attributes	
	RFC 2716 PPP EAP-TLS	
	RFC 2865 RADIUS Authentication	
	RFC 2866 RADIUS Accounting	
	RFC 2867 RADIUS Tunnel Accounting	
	RFC 2869 RADIUS Extensions	
	RFC 3576 Dynamic Authorization Extensions to RADIUS	
	RFC 3579 RADIUS Support for EAP	
	RFC 3580 IEEE 802.1X RADIUS Guidelines	
	RFC 3748 Extensible Authentication Protocol	
	Web-based authentication	
	TACACS support for management users	
	RFC 854 Telnet	
	RFC 1155 Management Information for TCP/IP-Based Internets	
	RFC 1156 MIB	
	RFC 1157 SNMP	
	RFC 1213 SNMP MIB II	
	RFC 1350 TFTP	

	RFC 1643 Ethernet MIB	
	RFC 2030 SNMP	
	RFC 2616 HTTP	
	RFC 2665 Ethernet-Like Interface types MIB	
	RFC 2674 Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual Extensions	
	RFC 2819 RMON MIB	
	RFC 2863 Interfaces Group MIB	
	RFC 3164 Syslog	
	RFC 3418 MIB for SNMP	
	RFC 3636 Definitions of Managed Objects for IEEE 802.3 MAUs	
	Enterprise private MIBs	
	Other Specifications	
9	WLANs (BSSIDs): 144	
	Profile Groups per Controller: 9 (1 Basic + 8 Advanced)	
	Profile per Controller: 128	
	Security Profile Groups per Profile Group: 9 (1 Basic + 8 Advanced)	
	Radius, AD, and LDAP proxy	
	Rate Limiting on per SSID and per Client	
	Schedule AP on/off	
	Stacking Redundancy (N+1)	
	IPv4 and IPv6 support	
	VLANs: 64+1 Management	
	Active-standby Redundancy	
	DHCP Server	
	Environmental Conditions	
10	Operating Temperature: 0° to 45°	
	Storage Temperature: -20° to 70°	
	Operating Relative Humidity: 10% to 90%	
	Storage Humidity: 5% to 95%	
	MTBF: 664,072 hours minimum	
	Power Consumption: 13W maximum	
	Licenses for AP Management	
11	Only once Licenses need to be taken, Renewal not require	
	Approved Make: Cisco /Sophos /Dell/Netgear	
	Warranty and Support	
12	Lifetime free latest firmware support	
	Replacement with New Product Only No refurbished Products.	
S. No.	Minimum Required Specifications	Compliance Yes/No

Item	24-port Gigabit managed switch with smart PoE and 4-ports IG SFP	
2.	Physical Specifications	
	i. 24 x 10/100/1000 Base-T auto-sensing PoE ports	
	ii. 2 dedicated 100/1000 Base-X Fiber SFP ports	
3.	Performance Specification	
	i. Bandwidth: 52 GBps non-blocking	
	ii. Forwarding modes: Store-and-forward	
	iii. 8 Priority queues	
	iv. Weighted Round Robin (WRR) and Strict Priority	
	v. MAC Address database size 8000 media access control (MAC) addresses	
	vi. VLAN 256	
	vii. 128 Multicast groups	
	viii. Number of DHCP snooping binding;s: 256	
	ix. Packet forwarding rate (64 byte packet size) 38 Mpps	
	x. Jumbo frame support: Up to 9K packet size	
	xi. Auto Power Down	
	xii. PoE budget 190W	
	xiii. PoE Timer & Power Management	
4.	IEEE Network Protocols	
	i. IEEE 802.3 Ethernet	
	ii. IEEE 802.3u 100BASE-T	
	iii. IEEE 802.1Q VLAN Tagging	
	iv. IEEE 802.3ab 1000BASE-T	
	v. IEEE 802.3af PoE	
	vi. IEEE 802.3at PoE+	
	vii. IEEE 802.3az Energy Efficient Ethernet (EEE)	
	i. IEEE 802.3ad Trunking (LACP)	
	ii. IEEE 802.3z Gigabit Ethernet 1000BASE-SX/ LX	
	iii. IEEE 802.3x Full-Duplex Flow Control	
	iv. IEEE 802.1AB LLDP with ANSII/TIA-105 7 (LLDP-MED)	
	v. IEEE 802.1p Class of Service	
	vi. IEEE 802.1D Spanning Tree (STP)	
	vii. IEEE 802.1s Multiple Spanning Tree (MSTP)	
	viii. IEEE 802.1w Rapid Spanning Tree (RSTP)	
	ix. IEEE 802.1X Radius network access control	
5.	Network Security and Traffic	
	i. Guest VLAN	
	ii. RADIUS-based VLAN assignment via .1x	
	iii. RADIUS accounting	
	iv. Network Storm Protection	
	v. DoS attacks prevention	
	vi. Broadcast, Unicast, Multicast Protection	
	vii. Access Control Lists (ACLs) L2 / L3 / L4	
	viii. IP-based ACLs (IPv4 and IPv6)	

	xvi. Auto-VoIP : Yes, based on protocols (SIP, H323 and SCCP) or on OUI bytes (default database and user-based OUIs) in the phone source MAC address	
	x. TCP/UDP-based ACL	
	xi. MAC lockdown	
	xii. MAC lockdown by the number of MACs	
	xiii. IEEE 802.1x Radius Port Access Authentication	
	xiv. Control MAC # Dynamic learned entries: 600	
	xv. Control MAC # Static entries :20	
6.	L2 Services	
	i. IEEE 802.1Q VLAN Tagging	
	ii. Video VLAN	
	iii. Voice VLAN	
	iv. IEEE 802.3ad - LAGs - LACP ((8 LAGS with max. of 8 members in each LAG))	
	v. Broadcast Storm Control	
	vi. IGMP Snooping (v1, v2 and v3)	
	vii. IGMP Snooping queriers	
7.	Network Monitoring and Discovery Services	
	i. 802.1ab LLDP	
	ii. SNMP V1, V2, V3	
	iii. RMON 1,2,3,9	
8.	QoS	
	i. Port-based rate limiting	
	ii. Port-based QoS	
	iii. DiffServQoS	
	iv. IEEE 802.1p COS	
	v. IPv4 DSCP	
	vi. Diff ServQoS	
	vii. IPv4 ToS	
9.	Management	
	i. Password management	
	ii. Configurable Management VLAN	
	iii. Admin access control via Radius and TACACS+	
	iv. Web-based graphical user interface (GUI)	
	v. Smart Control Center (SCC) for multiswitch management	
	vi. IPv6 management	
	vii. Dual Software (firmware) image	
	viii. Dual Configuration file	
	ix. SNTP client over UOP port 123	
	x. SNMP v1/v2	
	xi. SNMP v3 with multiple IP addresses	
	xii. RMON 1,2,3,9	
	xiii. Port Mirroring	
	xiv. Many to One Port Mirroring	
	xv. Cable Test utility	
	xvi. SSL/HTTPS and TLS v1.0 for web-based access	

	xvii. TFTP/HTTP File transfers (uploads, downloads)	
	xviii. HTTP Download (firmware)	
	xix. Syslog (RFC 3164)	
10.	Certification	
	i. CE mark, commercial	
	ii. FCC Part 15 Class A, VCCI Class A	
	iii. Class A EN 55022 (CISPR 22) Class A	
	iv. Class A C-Tick	
	v. EN 50082-1	
	vi. EN 55024	
	vii. CCC	
	viii. CSA certified (CSA 22.2 #950)	
	ix. UL listed (UL 1950)/cUL IEC 950/EN 60950	
	x. 47 CFR FCC Part 15, SubpartB, Class A	
	xi. ICES-003: 2016 Issue 6, Class A	
	xii. ANSI C63.4:2014	
	xiii. IEC 60950-1:2005 (ed.2)+A1:2009+A2:2013	
	xiv. AN /NZS CISPR 22:2009+A1:2010 CLASS A	
11.	Safety	
	i. AN/NZS 60950.1:2015	
	ii. IEC 60950-1:2005 (ed.2)+A1:2009+A2:2013	
	iii. EN 60950-1: 2006 + A11:2009 + A1:2010 + A12:2011 + A2:2013	
	iv. CSA certified (CSA 22.2 #950)	
	v. CCC (China Compulsory Certificate)	
	Approved Make: CISCO/DELL/ JUNIPER /EXTREME NETWORK /NETGEAR	
12.	Warranty and Support	
	Lifetime free latest firmware support	
	Replacement with New Product Only No refurbished Products.	
Item No.	Minimum Technical Specifications	Compliance Yes/No
1	Technical Specification of Next-Gen Firewall UTM for 500 Users	
1	UTM should be multi core 64bit processor based modular architecture, should not be any proprietary ASIC based solution.	
2	Firewall Throughput: 48 GBps or better	
3	IPS Throughput: 10 GBps or better	
4	Anti-Virus Throughput: 6 GBps or better	
5	Concurrent Sessions: 20 Million or better	
6	New Sessions/connections per second: 200,000	
7	NGFW Throughput: 7.2 GBps or better	

8	Minimum 16 GB or more RAM	
9	Network Interfaces ports should have 8 Nos of 10/100/1000BaseT Ports, 2 x 1GbE SFP and 2 x 10GbE SFP+, 2 nos 40Gig QSFP+ ports and transceiver should be Populated 2 x 10 Gig SFP+ MM and 2 x 40Gig QFP+ MM from day-1.	
10	Internal Storage: 240 Gb SSD with RAID or higher along with Hot Swap Redundant Power Supply	
11	Shall support 802.1Q VLANs	
12	Shall support deployment in Active-Active HA mode and state full failover with Multiple ISP Link Aggregation Support (minimum 4 nos.)	
13	Shall provide IPSEC, L2TP VPN in the same appliance	
14	Shall provide state full firewall, integrated GUI access, auto backup option.	
15	Shall provide Gateway Anti-Virus & Anti - Malware with capability to scan, detect, remove and/or quarantine packets infected with Virus, Trojan, worms, etc.	
16	Shall provide spam filtering based on RBL checks, IP address blacklists, subject line and MIME header and provide facility to quarantine or redirect spam or suspected spam mails to a designated address.	
17	Shall support source and destination NAT, NAT Traversal for Voice protocols.	
18	Shall have protocol anomaly detection and support IPS signatures with provision for regular updates.	
19	It shall be possible to define custom IPS policies.	
20	Shall provide Application and web filtering features	
21	Shall support filters/policies based on user identity, IP address, MAC address.	
22	Shall support configuration of different security zones and apply access control policies/filters based on zones.	
23	Shall provide mechanisms to detect and protect from DoS, DDoS attacks and spoof	
24	Shall have capability to filter websites various categories including URL, keywords, file/MIME type as well as custom categories/keywords and block pages suspected of containing phishing and/or pharming links	
25	Shall support active-active & active-passive high availability	
26	Shall be capable of providing application security based on application categories including - P2P, Gaming, Internet Proxies. Etc.	
27	Shall support web application protection by preventing common application based threats.	
28	Shall provide mechanism to control and block instant messaging clients including prevention of IM based file transfers.	
29	The solution should have 6 GBps of VPN throughput and shall support minimum 200 clientless SSL VPN tunnels from day one without any extra cost.	
30	Shall support DES, 3DES, AES encryption along with SHA-1, MD5 authentication	
31	Shall support RIPv1&v2, OSPF, BGP and policy based routing, and Multicast Routing PIM,IGMP	

32	Shall support user/category/application/IP based bandwidth management and load balancing	
33	Shall support time based access control, Data transfer quota,	
34	Shall support local authentication server as well as integration with LDAP/Active Directory and RADIUS Servers	
35	Shall support DHCP Relay, NTP/SNTP, SNMP, Syslog	
36	It shall support management through web based GUI and CLI by way of serial console, Telnet and SSH.	
37	Shall support logging, viewing and reporting of all UTM services including firewall, IPS, Web & Application control, Anti-Virus etc.	
38	Solution should have option to work along with Endpoint to provide synchronized security	
39	Solution should have an option to work along with endpoint for synchronized apps detection and control	
40	The solution should be quoted with 100 Endpoint protection license for synchronized security	
41	Firewall should able to block anonymous proxy application (ultrasurf ,Tor etc.)	
42	The next generation firewall should support dual anti malware engine from day one	
43	Should support malicious traffic detection to protect any command and control connections for infected servers.	
44	Should have Web application firewall to manage 10 servers from cross site scripting, Sql injection etc.	
45	Should have reverse proxy, SSL offloading, form hardening, URL tempering protection	
46	Solution should have protection against Zero day/unseen malwares, should have local or cloud sandboxing platform for dynamic analysis of new/unseen file in any platform. The sandboxing should have use ML engine and should provide details reports of each & every file.	
47	The solution should have email protection in proxy & MTA mode. Should have inbuilt email DLP with content control list. Must support end to end email encryption without additional software.	
48	Shall include three years warranty for the appliance along with license & subscription for Gateway Antivirus, Advance Threat prevention, Web / URL Filtering, content and application filtering, Email protection, Cloud sandboxing, Web Application Firewall and IPS. License period will be counted after activation. 24X7 warranty and support from OEM	
49	Certification ICSA Firewall - Corporate	
50	OEM should be leader in Gartner UTM Magic Quadrant for last 3 years	
51	Server Protection: Server protecting license including , PUA, Exploit Protection, Server Lockdown, Deep Learning , crypto guard ransom ware protection should be provide for 10 servers	
52	Approved Make: Cisco /Sophos /Fortinet /Juniper	
53	Third-Party or same OEM ssl certificate required :-	

	Web server cert . Secure site EB Wildcard with 256-bit Encryption secure unlimited sub domains, Validity would be 3 years, Comes with Daily basis malware scanning, Supports all major browsers such as Mozilla, Internet Explorer, Chrome and all Android & windows Mobile devices.	
	Secure Mail server certificate : Include pop, imap, smtp & url, Validity would be 3 Yrs, Encryption up-to 256bit, Provide free of cost unlimited reissuance throughout the span of certificate, Supports all major browsers such as Mozilla, Internet Explorer, Chrome and all Android & windows Mobile devices.	
54	1 Years 24 X 7 Support. The bidder must enclose along with Technical Bid OEM authorization specific to this tender, and technical compliance duly approved by the OEM, failing which the Bid offer will be rejected.	
Item No.	Minimum Technical Specifications	Compliance Yes/No
Technical Specification of Next-Gen Firewall UTM for 250 Users		
1	Industry Certifications and Evaluations	
1.1	Firewall solution offered from OEM must be rated as ‘Leaders’ in the latest Magic Quadrant for UTM published by Gartner in last three years (2016, 2017, 2018)	
1.2	Solution should have ICSA certification for Firewall	
2	Hardware Architecture	
2.1	The appliance based security platform should be capable of providing firewall, application visibility, Web Protection and IPS functionality in a single appliance	
2.2	The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support minimum 64GB memory. Should not be any proprietary component such as ASIC.	
2.3	The appliance should support at least 8 * (1G) ports, 2*1G SFP and 2 * 10 G SFP+ ports from day 1 & 2 * 40G ports for future extension.	
3	Performance & Scalability	
3.1	Should support atleast 32 GBps Firewall throughput & 5 GBps of NGFW throughput (includes FW, Application control & IPS)	
3.2	Proposed appliance should support atleast 16 million concurrent sessions or more	
3.3	Firewall should support at least 200K connections per second or more	
3.4	Firewall Should support atleast 8 GBps of IPS throughput or more	
3.5	Firewall Should support atleast 5 GBps of AV throughput or more	
3.6	NG Firewall should support atleast 1000 VLANs	
4	High-Availability Features	
4.1	Firewall should support Active/Standby or Active/Active/Clustering failover	
4.2	Firewall should support Link Aggregation functionality for the failover control & date interfaces for provide additional level of redundancy	
4.3	Firewall should support redundant interfaces to provide interface level redundancy before device failover	
4.4	Firewall should have 180 GB SSD internal Storage Capacity	
4.5	Firewall should have optional redundant power supply	
5	NGFW Firewall Features	
5.1	Should support Static, RIP, OSPF and BGP, &Multicast protocols like IGMP, PIM, etc	
5.2	Firewall should support manual NAT and Auto-NAT, static nat, dynamic nat, dynamic pat	

5.3	Full configuration of DNS, DHCP and NTP,802.3ad interface link aggregation Dynamic DNS,IPv6 support ,Upstream proxy support	
5.4	Should support capability to limit bandwidth on basis of user/IP/apps / groups, Networks / Ports, URLEtc	
5.5	Advanced Threat Protection (Detect and block network traffic attempting to contact command and control servers using multi-layered DNS, AFC, and firewall)	
5.6	Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies on more than 100 million of URLs in more than 90 categories.	
5.7	Should have a option for dual antivirus engine one must be from gartner leader quardant AV vendor	
5.8	Malware scanning: block all forms of viruses, web malware, trojans and spyware on HTTP/S, FTP and web-based email	
5.9	Advanced web malware protection with JavaScript emulation,Pharming Protection and cloud sandboxing for zero day analysis	
5.1	Should support more than 6000 application layer and risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.	
5.11	High-performance, next-gen IPS deep packet inspection engine with selective IPS patterns for maximum performance and protection	
5.12	The detection engine should support the capability of detecting variants of known threats, as well as new threats	
5.13	The solution should have ability to instantly identifies compromised endpoints including the host, user, process,incident count, and time of compromise	
5.14	The solution should have a option to limit endpoint access to network resources or completely isolate compromised systems until they are cleaned up	
5.15	The solution should automatically protects healthy systems from connecting to compromised endpoints , 50 endpoint license should be quoted along with EDR & zero day ransomware protection capability	
5.16	The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).	
5.17	The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioral anomaly detection techniques. Identify and explain each type of detection mechanism supported.	
5.18	The solution should have inbuilt web appliacation firewall to protection against Reverse proxy,SQL injection protection,Cross-site scripting etc.	
5.19	The solution should support URL hardening engine with deep-linking and directory traversal prevention	
5.2	Solution should support HTTPS (SSL) encryption offloading,Cookie signing with digital signatures	
5.21	Should support Path-based routing and reverse authentication (offloading) for form- based and basic authentication for server access	
5.22	E-mail scanning with SMTP, POP3, and IMAP support TLS Encryption for SMTP, POP and IMAP	
5.23	File-Type detection/blocking/scanning of attachments,Detects phishing URLs within e- mails	
5.24	Spam quarantine digest and notifications options,Self-serve user portal for viewing and releasing quarantined messages	
5.25	DLP engine with Pre-packaged sensitive data type content control lists (CCLs) automatic scanning of emails and attachments for sensitive data	

5.26	The solution should work as MTA & should have end to end SPX encryption capability	
5.27	The solution should offerd with onprem/cloud sandboxing subscription to combat against zero day unknown threats	
5.28	The solution should offered machine learning capability in sandboxing capability	
5.29	The solution should have unlimited number of Ipsec&SSI VPN client free of cost	
5.3	The solution should support VPN with Remote Ethernet Device by zero touch deployment	
6	Management & Logging	
6.1	The management platform must be accessible via a web-based interface and ideally with no need for additional client software	
6.2	Solution should include troubleshooting tools like Packet tracer, capture	
6.3	The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.	
6.4	The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.	
6.6	Compliance reports (HIPAA, GLBA, SOX, FISMA, PCI-DSS, NERC CIP v3, and CIPA)	
6.7	Approved Make: Cisco /Sophos /Fortinet /Juniper	
S. No.	Minimum Required Specifications	Compliance Yes/No
	Make: Model/ Part No.	
1 KVA Line Interactive UPS		
1	Back Up 30 Min on full load	
2	2 Battery 2 X 14 AH	
S. No.	Minimum Required Specifications	Compliance Yes/No
	Make: Model/ Part No.	
SM Fiber optic Cable		
1	Cable Type Single Mode, OS2, Armored, Loose Tube – Unitube, CSTA, Jelly Filled	
2	No. of cores 6	
3	Water blocking compound	
	Cable must have Water blocking compound	
4	Strength Member Should have FRP strength member	
5	Cable outer jacket Specification	
	Must have Dielectric and Metallic Sheath Cable. Cable must be direct buried	
6	Attenuation :	
	@1310nm <= 0.33 dB/Km	
	@1550nm <= 0.19 dB/Km	
	Coating / Cladding non-circularity <= 12 microns	
	Zero Dispersion Slope <= 0.092 ps / sqnm-km	
	Fiber core UL Listed	
	Tensile rating Not less than 1000N	
	Maximum Crush resistance Not less than 44N/mm	
	Armor Corrugated Steel tape Armor	

	Approval UL Listed Fiber	
	RoHS Compliant	
	Approved Make: Molex/ Dlink/ Digilink or Equivalent	

General Terms:

1. The technical specification should be quoted in same manner as described in the tender.
2. Each product should have at least three years warranty and after warranty CAMC for further 2 years should be provided by vendor. During warranty period as well as during Comprehensive Annual Maintenance Contract period, firm will maintain the system with all spares, PCB, accessories, electronics components, all type of consumables (including battery of UPS) etc.
3. The vendor should ensure quick back up response in case of equipment failure which should be replacing if needed within 10 days of the distress call.
4. Integration, installation and setup should be done by vendor. The quantity of the items may increase of decrease as per requirement during establishment of Wi-Fi network inside the hostel complex. Further, if some more areas is required to providing the said facility, the same may also be done based on the rates quoted by the bidder. Hence, rates to be quoted must be valid for a further period of one year i.e. up to March – 2021.
5. All compatible cables, cords, connectors and other accessories should be provided by vendor to integrate the Wi-Fi components.
6. Director, IGIMS, Patna reserve the right to purchase either all the items mentioned in BOQ or some parts as per requirement and availability of funds for the said purposes.



**Director,
IGIMS, PATNA**

COMPLIANCE STATEMENT

INDIRA GANDHI INSTITUTE FOF MEDICAL SCIENCES, PATNA (BIHAR)

Ref: - Tender Notice No.:

S. NO.	Check list of documents/ Undertakings?	YES/NO (Mention page no. of Technical Bid, where supporting documents are attached.)	Remarks (Give explanation if answer is No)
1	Is Tender fees attached?		
2	Is EMD attached? (if applicable)		
3	Is the bidder original equipment Manufacturer (OEM) / authorized dealer?		
4	If authorized dealer, recent dated Certificate to this effect from OEM, attached or not?		
5.	Undertaking from OEM regarding technical support & extended warranty period		
6.	Undertaking from bidder regarding acceptance of tender terms & conditions		
7.	Whether list of reputed users (along with telephone numbers of contact persons) for the past three years specific to the instrument attached.		
8.	Whether special educational discount for Indira Gandhi Institute of Medical Sciences, Sheikhpura, Patna given.		
9.	Does the instrument complies with all the required specifications as per Annexure 1. Attach a separate sheet showing compliance with the specifications and explanations thereto if the equipments varies from the requested specifications.		
10.	Whether free Installation, Commissioning and Application Training offered.		
11.	Whether Comprehensive Annual maintenance after expiry of comprehensive onsite warranty quoted separately.		

Annexure – D


S.N.	Description	Quantity	Unit	Unit Price	GST Tax @ 18%	Unit Price With GST	Amount with GST
Supply Installation Testing & Commissioning Wi-Fi Access Point.							
1	Dual Band Wireless-AC Access Point Approved Make: Cisco /Sophos /Dell/Netgear	50	PCS				
2	High Performance Enterprise-Class Wireless Controller with 50 AP Support Approved Make: Cisco /Sophos /Dell/Netgear	1	Each				
3	24-port 10/100/1000 Base-T Gigabit PoE+ Managed Switch Approved Make: CISCO /DELL/ JUNIPER /EXTREME NETWORK /NETGEAR	5	Each				
4	1000BASE, SM Module connector Approved Make: Cisco /Sophos /Dell/Netgear or Equivalent	8	Each				
5	UTM for 500 User with 3 years Subscription - Type A Approved Make: Cisco /Sophos /Fortinet /Juniper (Optional Item)	1	Each				
6	UTM for 250 User with 3 years Subscription - Type B Approved Make: Cisco /Sophos /Fortinet /Juniper	1	Each				
7	CAT-6 Cable (box)@ 305 Mtr. Approved Make - Commscope/ Molex / Dlink/Amp	4	Box				
8	6 Core ARMOURED S.M.OFC Approved Make - Commscope/ Molex / Dlink/Amp	500	Mtr				
9	9U RACK with PDU and cable manager, MCB 32 AMP (DP) for each rack, Make - OEM Recommended	6	Each				
10	1 KVA Line Interactive UPS, Make – Delta / Vertiv or Equivalent	6	Each				
11	CAT 6 Patch Pannel Approved Make - Commscope/ Molex / Dlink/Amp	6	Each				

12	CAT 6 1 mtr Patch chord , Approved Make - Commscope/ Molex / Dlink/Amp	100	Each					
13	CAT 6 I/O with complete set, Approved Make - Commscope/ Molex / Dlink/Amp	50	Each					
14	Laying of CAT-6e UTP and respective accessories (with PVC Conduit / Casing)	1200	Mtr					
15	Laying of OFC with respective accessories (including underground laying with HDPP conduit with depth of 1 M)	500	Mtr					
16.	Supply installation and commissioning of Above Items	1	Job Work					
17.	ILL Connection							
	Supply of 50 Mbps, (1: 1) ILL Connection through Fibre in Ring topology for 3 year subscription, Make -OEM	1	No.					
Total								

Warranty Period:	Three Years
1st Year CAMC Charges after expiry of warranty period: (with out GST)	
2nd Year CAMC Charges after expiry of warranty period: (with out GST)	

Remarks:

- **Technical Bid should contain** Annexure – A (Bid Particulars), Annexure – B (Technical Compliance Sheet), and Annexure – C (Compliance Statement) with all supporting documents.
- **Financial Bid should contain** only price in the format as per Annexure – D (BOQ).


Director,
I.G.I.M.S. – Patna.
