INDIAN INSTITUTE OF SCIENCE, BANGALORE

OPEN TENDER

Supply, installation, and commissioning of Wireless LAN Access Infrastructure at hostels of Indian Institute of Science, Bangalore

Tender No: IISc / TINA / 11 / 2019 Date: 20th Nov 2019

Telecom and Internet Access Committee
Indian Institute of Science
Bangalore 560012

November 2019

INDIAN INSTITUTE OF SCIENCE, BANGALORE

Tender No.: IISc / TINA / 11 / 2019 Date: 20th November 2019

TENDER DOCUMENT

Subject: Supply, installation, and commissioning of Wireless LAN Access Infrastructure at hostels of Indian Institute of Science, Bangalore.

INDEX

Schedule of Events

The tender document will be made available on the IISc website from the date of release of the tender.

Table 1: Schedule of Events

Release of Tender	November 20, 2019.
Site survey	November 26, 2019, 10.00 am IST
Deadline for submission of queries (for Prebid clarification):	November 28, 2019, 05.00 pm IST
Prebid clarification Meeting	December 4, 2019. 03.00 pm IST
Deadline for submission of bid	December 20, 2019, 05.00 pm IST
Opening of Technical bid	December 23, 2019, 03.00 pm IST
Technical presentations	December 26-27, 2019.
Listing of technically qualified bidders	To be declared later
Opening of price bids	To be declared later

No request for extension of any deadline will be entertained.

INTRODUCTION

Telecom and Internet Access Committee (TINA) at Indian Institute of Science (IISc) provides the Telecom, Internet and Network services to the Institute Community.
The core network infrastructure is currently located in the Supercomputer Education and Research Centre (SERC) and provides services to the Institute faculty, staff and students round the clock. The campus, having around 50 departments, is connected to the core infrastructure by a fiber optic backbone with active devices delivering Gigabit performance. The Institute is a part of the National Knowledge Network (NKN) of the Government of India and currently has 10Gbps Internet Bandwidth. In addition to this, the Institute also has Internet Bandwidth of 20 Mbps from a private provider.

The IISc Student Hostel blocks are spread out over some parts of the campus. At present, only few of the blocks are connected to the Institute network but almost none of them has Wi-Fi infrastructure. Interested bidders are invited to submit proposals for the supply, installation and commissioning of Access Points and switches for extending the Institute Wi-Fi network to the hostels.

SCOPE OF WORK:

The Institute invites proposals in a two-cover format from bidders who have the capability to provide a **TOTAL TURNKEY** solution which includes

(a) Supply,
(b) Transportation to the site,
(c) Transit insurance,
(d) Installation, including necessary cabling, testing, commissioning and documentation.
(e) Integration with the existing environment,
(f) Three years of comprehensive warranty, and
(f) Two years of post-warranty AMC.

Detailed technical scope of work and the technical specifications are mentioned in the subsequent sections. The bidders must ensure that the resources (personnel) allocated for each one of the above tasks are competent and capable of meeting all the technical requirements in order to ensure that the broad objective of delivery of services as per expectations is fully met. All correspondence with regards to this tender should be addressed to **The Chair, TINA, Indian Institute of Science, Bangalore – 560012, India (*wifitender.digits@iisc.ac.in*)** only.

BID SUBMISSION

BIDDER'S ELIGIBILITY CRITERIA

Compliance with the following conditions are mandatory.

1. The Wireless LAN Access Infrastructure (Wi-Fi & WIPS Solution) should have been implemented by the bidder (Tier-1 System Integrator (SI) partner of the OEM) in at least three centrally funded technical institutes (IITs/NITs) or Research labs (DRDO, CSIR, C-DAC, C-DOT, ERNET etc.), in the last three years. The value of any one turnkey solution implemented must be at least **Rs. 7 crores**. Complete list, along with the contact details of the customers (as mentioned above), must be provided.

Supporting Documents to be enclosed:

a)	Copies of the P. O.-s, stating clearly the duration of contract, value, and scope.	YES/NO
b)	Letter from the organization, supporting the claim of completion of the project and satisfactory delivery of services.	YES/NO
c)	Letter from the OEM to support the claim of Tier-1 relationship of SI with the OEM.	YES/NO

2. The bidder must have a registered office in India and been in operation for at least 10 years as on 31.03.2019. Joint venture or consortium are not permitted.

Supporting Documents to be enclosed:

a)	Documents supporting the above claim	YES/NO

3. The OEM must provide all technical support to the bidder for the contract period. A letter to this effect must be submitted along with the bid.

Supporting Documents to be enclosed:

a)	Authorization letter from the OEM to support SI during the contract period	YES/NO

4. The bidder is expected to be a profit-making company with an annual turnover of at least **Rs.100 Crores** in each of the last 3 financial years.

Supporting Documents to be enclosed:

a)	Annual audited balance sheets for 3 years	YES/NO

5. The bidder should be in a position to demonstrate its capability to deliver all the services expected during the contract period.

Supporting Documents to be enclosed:

a)	Documents supporting the above claim	YES/NO

6. The bidder must have an office in Bangalore with Service/Support Engineers posted in Bangalore.

Supporting Documents to be enclosed:

a)	Documents supporting the above claim	YES/NO

7. The bidder must not be blacklisted by Central Govt. /State Govt./PSUs/Other Govt. Agency/ Govt Educational Institute/University.

Supporting Documents to be enclosed:

a)	A declaration on company’s letterhead.	YES/NO

8. The bidder must submit Solvency Certificate of at least Rs. 50 Crores or above from Scheduled Commercial Bank. The Certificate should not older than 12 months.

Supporting Documents to be enclosed:

a)	Solvency Certificate from Scheduled Commercial Bank	YES/NO

9. The bidder is expected to do a site survey and submit detailed survey report along with implementation plan.

Supporting Documents to be enclosed:

a)	Detailed site survey report	YES/NO

EARNEST MONEY DEPOSIT (EMD)

1. All bidders must submit **Rs. 10 Lakhs** as bid security in the form of RTGS/NEFT transfer, the bidder must submit e-receipt as a proof of EMD submission along with the technical bid. Failure to comply with this requirement will result in rejection of the bid. The account details of IISc are provided in Annexure 5.
2. After the placement of the purchase order on the successful bidder, the EMD amount will be returned to the unsuccessful bidders without interest.
3. The EMD amount will be returned to the successful bidder after the Institute places a firm purchase order for the procurement and the successful bidder then submits a performance security/bank guarantee followed by its verification.
4. The bid must be valid for at least 180 days from the actual date of opening of the technical bid. Withdrawal of the bid within the period of validity will result in forfeiture of the EMD amount.

GUIDELINES

1. This tendering process is based on an e-tender through Central Public Procurement Portal (CPPP - https://eprocure.gov.in/eprocure/app). If a bidder submits a response to the e-tender, then it is assumed that the bidder accepts all the conditions specified in this document. Tender submitted through any other mode will not be entertained.
2. The submission consists of two parts: Technical Bid and Commercial Bid.
   - 2.1. Technical bid should contain:
     - 2.1.1. Supporting documents mentioned in the BEC and Overall Compliance Statement.
     - 2.1.2. Terms and conditions of the offer.
     - 2.1.3. Supporting technical material, including brochures.
     - 2.1.4. A duly filled technical compliance sheet as mentioned in Annexure 2 of the RFP.
     - 2.1.5. A duly filled BOQ compliance sheet as mentioned in Annexure 4 of the RFP. No prices should be mentioned.
   - 2.2. Commercial bid (Financial bid or Price Bid) should contain:
     - 2.2.1. The commercial bid must contain prices for every line item in the BOQ (Annexure 3).
     - 2.2.2. Any additional item over and above the items mentioned in Annexure 3 must be mentioned clearly as a separate line item, stating the quantity, unit of measurement and must be with 3 years of warranty.
     - 2.2.3. The final commercial evaluation will be based on Total Price of all the line items.

POINTS TO NOTE:

1. Prices should not be mentioned in the Technical Bid.
2. The supply of equipment and materials must be completed within 8 weeks from the date of the PO from IISc and the installation is to be completed within 6-8 weeks after supply of the equipment.
3. IISc is eligible for reduced customs duty for supply of equipment quoted in foreign currency; all such equipment must be shown as separate line items. Bidders planning to quote any imported solution must give the offer in the respective currency.
4. The offer must clearly state the components of pricing separately. For example, the supply part, F & I, I & C, Warranty services and any other charges must be quoted as separate line items.

5. A tender not complying with any of the above conditions is liable to be rejected. Incomplete proposals are liable to be rejected.
6. The Director, IISc, Bangalore-12 reserves the right to modify the technical specifications or the required quantity at any time. In such case, the bidders will be notified.
7. The Director, IISc reserves the right to accept or reject any proposal, in full or in part, without assigning any reason.
8. The bidders are requested to go through the Terms and Conditions detailed in this document, before filling out the e-tender.
9. A pre-bid clarification meeting is scheduled as per the timeline given later. Queries relating to the tender documents must be submitted in writing (Email address: ***wifitender.digits@iisc.ac.in***) on or before the specified timeline. Queries received after this deadline will not be entertained.

EVALUATION METHODOLOGY

The evaluation process to identify the successful bidder has two stages.

1. Evaluation of technical bids.

1.1. A technical committee constituted by the Institute will evaluate the submitted bids and identify the bidders that meet the mandatory technical requirements mentioned elsewhere in this document.

1.2. It is expected that bidder will carry out a site survey and submit a detailed survey report along with the implementation plan.

1.3. All bidders whose bids are found responsive will be invited for technical presentation at IISc. Schedule for the presentation will intimated via email correspondence.

1.4. The criteria set out for evaluation of the technical offer is given in Table 2.

Table 2: Bidder's Evaluation Criteria

Sl. No.	Description
1	Bidder’s Eligibility Criteria
2	Technical presentation and demonstration of a subset of features as desired by the technical evaluation committee

1.5. Technical presentation will be limited to 50 minutes, out of which 30 minutes must be spent on demonstration of features.

1.5.1. Presentation: 20 minutes

- SI company – 1 slide
- Special characteristics of the proposed solution – 3 slides
- Site survey report, thoughts on implementation – 4 slides

1.5.2. Demonstration of select features, Q&A: 30 minutes

1.6. The decision of the technical committee is final and binding on all the bidders.

2. Evaluation of commercial bids

2.1. Only technically qualified bidders’ commercial bids will be taken up for evaluation in the e-tendering process. Commercial bids shall be opened only for the technically qualified bidders after the technical evaluation. The Institute will communicate the date and time of opening of the commercial bids through CPPP portal.

2.2. Commercial bids which are not in compliance with the terms and conditions set out [Refer to “Commercial Terms and Conditions”] in the tender will be rejected.

2.3. For bids/components of bids submitted in foreign currency, the INR equivalent will be calculated using the exchange rate on the day of opening of the commercial bid.

ACCEPTANCE CRITERIA

1. The successful bidder must implement the solution at the site and complete the necessary integration of the solution with the core network infrastructure deployed at IISc and demonstrate the performance of the deployed infrastructure to the technical committee.
2. The bidder is expected to adhere to the Acceptance Test Plan (ATP) given in Annexure 1.
3. The warranty services will start only after installation and commissioning of the WLAN and WIPS solution.

SERVICE LEVEL AGREEMENT AND WARRANTY

1. In the event of failure of any of the sub-systems or components of the proposed solution, the bidder must ensure that defects are rectified, or the equipment is replaced with necessary configuration free of cost within 24 hours from the time it was reported.
2. Failure to meet the above requirement will result in extension of warranty services by 3 days for each day of delay during the warranty period.
3. The bidder must maintain a suitable stock of necessary spare equipment during the contract period.
4. The bidder must provide 3 years' warranty and thereafter 2 years' comprehensive AMC for all the hardware and software components of the solution, from the date on which the solution is accepted, as per the Acceptance Test Plan. During the warranty period and AMC period, the bidder must undertake comprehensive maintenance of all the equipment, hardware components, support and accessories. The bidder must also perform periodic software upgrades, updates, and patches, as well as preventive maintenance.
5. Collecting of faulty hardware from the site and provisioning the replacement hardware during the contract period (warranty & comprehensive AMC) on the site shall be the responsibility of the bidder.
6. IISc reserves the right to invoke the Performance Bank Guarantee submitted by bidder in case
   a. Supplied equipment, hardware & software components fail to achieve the performance as stipulated in this document.
   b. The bidder fails to provide satisfactory service in the scheduled time frame, during the contract period, as stipulated in this document.
7. The bidder should also clearly indicate post-warranty comprehensive AMC cost, covering all hardware and software upgrades, as a percentage of the equipment cost for a period of 2 years, on an annual basis, in the commercial bid.

COMMERCIAL TERMS & CONDITIONS

1. The commercial bid should contain among other things, payment terms, warranty, installation, commissioning, AMC charges etc. as per BOQ. All such conditions must be in line with the tender. In case of any deviation or conditional offer, the bid may be treated as non-responsive and hence will not be considered for evaluation. These charges will be paid only after successful supply, installation and acceptance. IISc will enter into a contract with the successful bidder which will detail all contractual obligations during the warranty period. Bidders must quote for AMC charges for two (2) years after the three (3) years warranty period.
2. IISc is registered with DSIR in order to get concession / exemption in Customs Duty / IGST (for import). Also, only 5% GST (for indigenous items) is applicable for IISc purchases as per DSIR registration. IISc will provide necessary documents required for availing concession / exemption in Customs Duty / IGST for import and 5% GST for indigenous items. Bidders should consider these facts while offering their price bids for this tender. Please note that IISc will not be involved in custom duty / airport charges payment, custom clearance, forwarding and transportation / shipment of import items; IISc will only provide relevant documents for availing concession / exemption in Custom duty / IGST subject to submission of documents (viz. Invoice, Bill of Entry, Bill of Lading, airway Bill, etc.) by the vendor. Bill of Entry must be in the name of IISc. Customs duty must be paid by the vendor only. Before release of final payment, all original documents with regards to import must be handed over to IISc, failing which final payment may not be released.
3. In case of rupee offer, the component of tax, and any other statutory levies should be shown separately and not included in the total amount, to enable us to avail exemption.
4. In case of imports, the commercial bid should contain among other things, the name and address of the Indian agent, if any, and the agency commission payable to the agent. Please quote the prices for import items on 'DDP - Delivered Duty Paid' terms.
5. Proposals should contain the name and contact details, viz., phone, fax and email of the designated person to whom all future communication will be addressed.
6. Prices should be quoted in detail, for all the subsystems given in the Technical Specifications part of the tender. Further, price validity should be for six months.
7. IISc will place the purchase order only on the successful bidder.

PAYMENT TERMS

1. The total project cost will consist of two parts
   1.1. Equipment supply part (Supply).
   1.2. Installation, testing, commissioning, documentation, warranty and AMC charges / maintenance services part (referred to as "Services" in short).
2. Payment Terms: - Payment will be released as follows:
   2.1. For orders placed in foreign / INR currency, payment towards 80% of the total order value of the Supply part will be released only after delivery of all such items on site at IISc, Bangalore, followed by inspection and auditing by the IISc Committee and submission of report regarding delivery of correct items by the Committee. Rest of the amount (20% of the order value of Supply and 100% of Services) will be paid only after completion of installation, commissioning, Acceptance Test Plan (ATP) and acceptance by the IISc Committee, followed by submission of a report regarding completion of the work by the Committee. Payments will be released through RTGS only (*no payment through Letter of Credit (LC)).*
   2.2. Services part of the project is payable only in Indian Rupees and will be paid only after completion of installation, commissioning, Acceptance Test Plan (ATP) and acceptance by the IISc.
   2.3. At the time of installation, any additional requirement of Supply or Services, over and above the quantity mentioned in the attached BOQ must be supported at the same rate as originally quoted.
   2.4. At the time of installation, if additional or less quantity of various items of Supply or Services are needed, then payment will be released only for actual Supply and Services. Final payment will be adjusted accordingly. Any payment will be released only after submission of PBG followed by receiving of verification report of genuineness of the Bank Guarantee.
   2.5. Payment will subject to deduction of TDS as per rules/laws.
   2.6. After completion of the warranty period, AMC charges will be paid once in every six months after completion of six-month AMC period, subject to a report of satisfactory performance by the user department of IISc.
3. Performance Security / Performance Bank Guarantee (PBG) – After placement of order, the successful bidder must submit Performance Security / Performance Bank Guarantee (PBG) within two weeks of the issue date of the order, failing which order may be cancelled. The PBG will be 10% of the total order value. The performance security must be valid for five years and two months from date of successful installation accepted by IISc. Performance security may be furnished in the form of RTGS / NEFT payment issued by a scheduled commercial bank in India (preferably nationalized bank) in favour of "The

Registrar, Indian Institute of Science, Bangalore." Bank details of IISc are attached in Annexure 5. No interest will be payable by IISc on the Performance Security deposited. The Earnest Money Deposit (EMD) of the successful bidder shall be returned on receipt of Performance Security (Performance Bank Guarantee / PBG). If the successful bidder fails to furnish the performance security or fails to deliver/provide the item/installation/service as per the order's terms and conditions within the stipulated period, the EMD shall be liable to be forfeited. The Performance Security will be forfeited and credited to IISc's account in the event of a breach of contract by the successful bidder. An undertaking to this effect must be submitted by the bidder.

4. Indian Agency commission (IAC), if any, must be mentioned in the commercial bid and it will be paid only after satisfactory installation & commissioning.

ANNEXURE 1

TECHNICAL SPECIFICATIONS

1. **Technical Specification of Wired Section of the Solution**

1.1. All the proposed Switches must be manageable, of enterprise class (not small business) and of Cisco/Juniper/Extreme make only, with full-fledged Layer-2 functionality. Switches must be accessible via SSH/Telnet.

1.2. All Switches listed under S/No 2 and 3 of the attached BOQ must have 1G SFP ports with 10Gbps SFP+ uplink. The switch must have redundant power supply.

1.3. All Switches listed under S/No 4 and 5 of the attached BOQ must have 10/100/1000 Mbps UTP ports with 1Gbps SFP uplink.

1.4. All SFP+ and SFP transceivers listed under S/No 6 and 7 of the attached BOQ must be of the same make as the quoted Switches.

1.5. All interconnections between Switches must be via Single Mode Optical Fiber (OFC) (9/125µm) except for cases where up-link and down-link switches are housed in the same Network rack.

1.6. All passive components of the wired network for the project listed under S/No. 8 to 21 in the attached BOQ must be of COMMSCOPE/TYCO/SYSTIMAX/BELDEN make only.

1.7. All network racks listed under S/No 22 and 23 of the attached BOQ must be of Netrack/Valrack/Rittal make only.

1.8. All PVC ducts listed under S/No. 24 to 26 in the attached BOQ must be of LEGRAND/MODI/MK make only.

1.9. All outdoor OFC cabling must be routed via HDPE pipes of PE-63 or higher which must be at least 1.5 inches in diameter and bearing ISI marking that must be buried underground at least 3 feet deep from solid surface.

1.10. All indoor OFC cabling must be routed in PVC conduit bearing ISI marking as listed under S/No. 26 in the attached BOQ.

1.11. All indoor Cat 6 UTP cabling must be routed in PVC casing and capping with ISI marking as listed under S/No. 24 and 25 in the attached BOQ with numbered ferrule at both ends.

1.12. All electrical components listed under S/No. 31 and 32 in the attached BOQ must be of LEGRAND/BELKIN/GM make only.

1.13. All indoor electrical cabling must be routed in the same PVC conduit along with OFC as mentioned in the item 1.8 above.

1.14. All UPS listed under S/No. 28 to 30 in the attached BOQ must be of APC/EMMERSON make only.

1.15. All Batteries listed under S/No. 28 to 30 in the attached BOQ must be of AMARON/EXIDE make only.

1.16. All Power Cords used to connect to all active devices must be 3-pin, round pin 5/15 AMP Power Cord.

1.17. All UTP cabling must be labelled on both Jack Panel end and Access Point end. The label must have information about Floor Number, Information Outlet number, Access point location (room number where AP is installed).

1.18. All OFC cabling must be labelled on both LIU ends. The label must have information of both Uplink and Downlink location, Floor number and room number.

1.19. All visible cables and patch cords must be neatly dressed and a routed in an orderly manner.

1.20. All road crossings must be via horizontal directional drilling (HDD).

2. Technical Specification of Wi-Fi and WIPS of the Solution

2.1. The proposed Controller and Access Points must be of Cisco/HPE(Aruba)/Arista make only.

2.2. The Wi-Fi Access Points should have a total of 3 or more radios, of which at least two should be dedicated 2x2 MU-MIMO radios for Wi-Fi access on both 2.4 GHz and 5 GHz bands, and at least one dedicated radio for WIPS and automatic channel allocation, operating simultaneously in a single device.

2.3. The solution must support wireless intrusion prevention system (WIPS) without effecting Wi-Fi performance.

2.4. Apart from DC power, the Wi-Fi Access Points and WIPS must work with all features supported on 802.3at PoE+.

2.5. Wi-Fi Access Points and the solution must support the following protocols: IEEE 802.11a/b/g, IEEE 802.11n, IEEE 802.11ac (WAVE 2), IEEE 802.11h, IEEE 802.11d, 802.11i.

2.6. The Wi-Fi Access Points devices and the solution should support the following authentication methods: 802.1X support, per-session encryption keys (WPA2).

2.7. Wi-Fi Access Points and WIPS should be remotely upgradeable from the controller, so that new features / upgrades can be added.

2.8. Wi-Fi Access Points should be approved by the Wireless Planning Commission (WPC).

2.9. Wi-Fi Access Points should have two-way band steering (example from 2.4GHz band to 5GHz and from 5 GHz to 2.4 GHz).

2.10. Wi-Fi Access Points should facilitate auto channel allocation to avoid interference between APs.

2.11. Wi-Fi Access Points and the solution should support configuration in both Bridge and NAT modes.

2.12. Wi-Fi Access Points and the solution should support 802.1Q VLANs. Further it should be possible to set Trunk Ports on Access Points.

2.13. Wi-Fi Access Points should support configurable management VLAN (support other than VLAN-1 as management VLAN).

2.14. Wi-Fi Access Points should be ceiling mountable.

2.15. Supply should include as many ceiling mountable units as the number of Access Points quoted.

3. Architecture of WLAN and WIPS

3.1. Proposed Wi-Fi management solution shall be a scalable cloud based for central management of all Wi-Fi and WIPS functionality. Further, it should support remote replication w.r.t DR.

3.2. Solution must support intelligent edge architecture for Wi-Fi access and wireless intrusion prevention (WIPS). All WLAN services should be delivered at the edge, eliminating the dependency on the controller i.e. all Wi-Fi & WIPS services should be functional on the device even if the link between AP and its management controller or the controller itself goes down.

3.3. The solution must facilitate Control and Provisioning of Wireless Access Point devices and ensure data encryption between access point devices and controllers across WAN/LAN links.

3.4. Wi-Fi controller should support deployment of set policies across the Wi-Fi AP devices placed on different network segments over LAN and WAN.

3.5. The Controller and Access Point device should support dual stack for IPV4 and IPV6.

3.6. Wireless manager solution must be PCI DSS and FIPS140-2 certified.

3.7. The solution should be able to work in a heterogenous environment by not hindering the operation of existing APs of different makes already deployed at IISc.

4. Wi-Fi Management

4.1. The Wi-Fi management controller should be cloud based with High Availability.

4.2. The solution must provide centralized Wi-Fi and WIPS management of the entire solution for both Wi-Fi and WIPS.

4.3. Quote should include all required Hardware and Software licenses to support all the Access Points and WIPS as listed under S/No. 1 of the attached BOQ. There should not be any additional licenses required for DR.

4.4. The solution must be scalable to support up to 2000 Access points and WIPS.

4.5. The solution must be able to simultaneously broadcast multiple SSIDs (at least 4) as visible network to client.

4.6. The solution should have the ability to create customizable dashboards.

4.7. The solution should have all-locations-consolidated dashboard and location-specific dashboard as well.

4.8. Solution should have role-based admin rights.

4.9. The solution must have policy-based management and administration.

4.10. The solution should detect and identify all types of Wi-Fi enabled client devices.

4.11. The solution must provide forensic data aggregated for major threat vectors like Rogue AP, Honeypot AP, Mis-Configured AP, DoS, Unauthorized Association, Ad Hoc Networks, Bridging/ICS Client, Mis-Association.

4.12. The solution should provide real-time RF coverage maps for the managed APs to help estimate RF coverage and leakage.

4.13. The solution should locate wireless devices (APs and Clients) accurately on floor maps.

4.14. The solution must provide location tracking of a DoS attacker.

4.15. Both the controller and Wi-Fi device should support SNMP v2c, v3.

4.16. The solution should support Captive Portal.

4.17. The solution should support External Splash Page.

4.18. The solution should support RADIUS, Active Directory and LDAP based authentication for both Corporate as well as Guest Clients.

4.19. The solution should support “Walled Garden” or equivalent feature for Guest Network.

4.20. The solution should support URL redirection.

4.21. The solution should provide Guest Client association time-out.

4.22. Solution should allow blocking of Guest user for specific time frame between two active sessions.

4.23. The solution should provide remote packet capture for troubleshooting.

4.24. The solution should support manual and automatic scheduling of system backup.

4.25. The solution should maintain logs which includes all activities performed by the users like login, any configuration changes made on the system, device deletion, device authorization, log out etc., for at least 365 days.

4.26. The solution should enable wireless client association analytics logs that includes client MAC address, AP connected to, data transfer, data rate, session duration, content - domain (http, https, IP address), for at least 180 days.

4.27. The solution should support uploading of all logs to external Syslog Server in LAN/WAN on real-time and scheduled basis.

4.28. The solution should provide application visibility. It should display list of applications with their data usage for a given SSID.

4.29. The solution should block traffic based on IP address, port, URL, hostname etc. and QoS (for example: bandwidth restriction for the SSID, QoS tagging of special traffic like Voice) at the edge (AP).

4.30. The solution must allow VLAN segmentation at the edge.

4.31. The solution must support Advanced Encryption Standards (AES), Temporal Key Integrity Protocol (TKIP).

4.32. Time Schedules - the solution must allow configuration of time schedules when WLAN is / is not available for a single or group of APs (For example: SSIDs can be active from 9 am to 5 pm and then automatically disabled and enabled).

4.33. The threat detection in the solution must be based on behavioural model (resilience against Zero-day attacks), in addition to signature based and threshold tuning.

4.34. The solution must have the capability of auto classifying Wi-Fi clients as authorized (managed clients connecting to IISc, Bangalore network), guest, rogue (un-managed client attempting connection to IISc, Bangalore network) or external (unmanaged not connecting to IISc, Bangalore network e.g. neighbour), in addition to manual classification.

4.35. The solution must indicate if it cannot reliably detect connectivity of Access Points.

4.36. The solution must be able to detect all types of Rogue (unauthorized APs connected to IISc, Bangalore network) Access Points.

4.37. The solution must detect mis-configured authorized Access Points.

4.38. The solution should be able to detect and prevent (if configured to do so) outside client trying to connect to the IISc, Bangalore network.

4.39. The solution should be able to detect and prevent (if configured to do so) all types of Ad-Hoc connections.

4.40. The solution must detect Honey Pot attacks including its advanced variants such as Multipot.

4.41. The WIPS solution should not affect the operation of other Access Points while preventing a rogue AP on the same channel.

4.42. The solution must be able to detect wireless Denial of Service (DoS) attacks.

4.43. Wi-Fi controllers License should work across subnets to reach Wi-Fi Access Points deployed in various network segments.

4.44. Wi-Fi controllers should support enforcing policies across multiple Access Points.

4.45. Wi-Fi controller should support both active / active and active / passive modes of operation.

5. Management and Monitoring

5.1. The solution should provide alerts in hierarchical structure.

5.2. The solution must send notifications based on location and alarm type.

5.3. The solution must support addition of tags and notes to devices.

5.4. The solution must provide a device summary (for APs and clients) report per location.

5.5. The solution must allow customization of existing reports and creation of new reports by an administrator.

5.6. The solution must allow automatic schedules for report generation and distribution of reports to specific users.

5.7. The solution should provide alerts for impact on WLAN performance such as:

5.7.1. High number of client association

5.7.2. Excessive frame re-transmission

5.7.3. Low average data rate for a client

5.7.4. Drop in a signal of an Access Point

5.7.5. Inadequate coverage

5.8. The solution should have built-in, make & model agnostic performance monitoring and Wi-Fi Analytics.

5.9. The controller and Wi-Fi AP devices management should support command line (SSH / telnet and as well as web based (HTTPS) administration.

6. Guest Management

6.1. Solution should allow enabling/disabling guest login features.

6.2. Solution should support multiple authentication mechanisms to authenticate guest users through a single captive portal, with an option of using any one or a combination (e.g.: Username and Password and/or SMS OTP) of authentication mechanisms.

6.3. Guest user should be able to authenticate with the Wi-Fi using a self-registration process, where the user will enter some requested information and an authorized person will check and approve the request and Wi-Fi access should be granted automatically post approval. For example: Solutions should support guest user authentication by SMS, social media, self-registration, where an authorized user can provide access to a guest after email verification.

6.4. The solution should support integration with SMTP server to send Wi-Fi access details via e-mail to guest users.

6.5. The solution should provide location-aware visitor, usage, loyalty, and social analytics information through different graphs of guest users.

6.6. The solution should provide the graphs that represent the data received, transmitted & total data exchange by days and location of guest users.

6.7. The solution should also provide various guest user management functions, such as importing and exporting guest user accounts and enabling and disabling guest user accounts.

6.8. The solution should be able to maintain profiles of the users connected to the guest Wi-Fi network; profiles should provide information such as login location, first name, last name, mobile number, last authentication time, email etc.

7. Coverage and Capacity Planning

7.1. On-site site survey by the bidder is required to plan Wi-Fi deployment in each floor of each building.

7.2. The solution must ensure at least -65 dBm RSSI inside all hostel rooms.

7.3. The bidder should provide the location of Access Points on the floor plan for all buildings (Note: tentative location plan will be provided by IISc).

7.4. The bidder should provide OEM-certified coverage heat map for 2.4 GHz and 5 GHz separately with -65 dBm RSSI threshold for 2.4 GHz. All coverage holes in the premises should be indicated clearly.

7.5. The bidder should provide OEM-certified AP coverage redundancy map.

8. License, Warranty and Support

8.1. The total solution should include licenses for all necessary features from the first day of the installation. All the licenses quoted should be perpetual. All the features and signatures including WIPS available at the time of expiration of license should continue to work. Renewal of licenses should be required only for new features and updates/releases announced by the OEM after the contract expires.

8.2. The total solution should have 3 years' on-site warranty for Access Points, Switches, UPS & batteries, cabling & accessories, and cloud-based controller subscription.

8.3. The total solution should include technical support for software/firmware and software upgrades for controller, Access Points and Switches for 3 years.

8.4. The total solution should be upgradable to the latest stable version, as and when available, at no extra cost.

8.5. The quote should also include additional 2 years' AMC specified as a separate line item.

8.6. Warranty support should include 4 hrs. response time and provision of replacement along with appropriate configuration and installation in next business day for Hardware.

8.7. Should provide single point of contact and should provide call logging and escalation matrix.

9. Acceptance Parameters for the Proposed Solution

9.1. Physical Installation:

9.1.1. Inspect installation of Network racks, OFC, UPS, Power Cables, UTP cables and Network Switches.

9.1.2. Configuration check on controller including the policies.

9.1.3. Test the physical mounting of each Access Point.

9.1.4. Test each Access Point connectivity to the central cloud-based controller.

9.2. Wired Network Test:

9.2.1. Perform OTDR/RFC 2544 tests for all OFC links and submit reports.

9.2.2. Perform end-to-end connectivity test of all UTP links and submit reports.

9.2.3. Check reachability and latency test on all Network Switches and submit reports.

9.3. Wi-Fi Controller Configuration Test:

9.3.1. Check authorized Wi-Fi set up for each Subnet / VLAN / Location as the case may be.

9.3.2. Check both Authorized user and Guest user policies.

9.3.3. Test each Access Point if they have the right authorized and guest policy.

9.3.4. Check Wi-Fi prevention policy for each subnet, VLAN and location.

9.3.5. Check the configured alerts and alert delivery methods.

9.3.6. Check the administrative users and their access rights.

9.3.7. Check the configured reports (content, delivery frequency, recipient list).

9.3.8. Check the automatic backup and archival parameters.

9.3.9. Check archival of logs.

9.4. Commissioning Test:

9.4.1. Test for all Access Points connectivity to the cloud-based controller.

9.4.2. Test and verify authorized Access Points inventory and authorized client inventory.

9.4.3. Verify external Access Points list and verify uncategorized / unauthorized client list.

9.4.4. Verify if all authorized wireless devices are tagged to right location.

9.4.5. Test for authorized client connection to authorized Access Point and respective SSID as per the set authentication policy.

9.4.6. Test for Guest client connection to authorized Access Points and respective SSID as per the set authentication policy.

9.4.7. Test if the Access Points are operational after shutting down the cloud-based controller.

9.4.8. Test if automatic Rogue Access Points prevention is working on all types of rogue APs.

9.4.9. Test if unauthorized client association to authorized Access Point is automatically prevented.

9.4.10. Test if automatic client Mis-association prevention is working.

9.4.11. Test if Ad-Hoc Networks are detected and automatically prevented.

9.4.12. Test if Mac-Spoofing is detected.

9.4.13. Test if automatic prevention of Honeypot (with Multipot) is functional.

9.4.14. Test is Denial of Service (DoS) Attack is detected.

9.4.15. Testing of deployment of policies, firmware updating remotely through the controller.

9.4.16. Testing WIPS functionality across the subnet.

9.4.17. The entire testing exercise should complete in two weeks' time from the Date of installation.

9.5. Documentation and Reports:

9.5.1. Documentation of the entire project along with testing reports must be submitted to IISc.

9.5.2. Documentation must include RF Coverage Heat Maps clearing showing that the -65 dBm RSSI requirement within all hostel rooms is met.

9.5.3. Documentation must include complete network diagram which clearly depicts Switch Management IP Address, Switch Location, AP Location and Switch Port to each AP.

9.5.4. Documentation must include complete configuration in a step-by-step manner.

9.6. Solution Fine Tuning and Handover to operations team of IISc Bangalore

9.6.1. Fine tune Wi-Fi Access policies and security policies

9.6.2. Rebuild authorized device inventory and remediate mis-configured APs.

9.6.3. Fine tune events, alerts, reports and other parameters.

ANNEXURE 2

TECHINICAL COMPLAINCE

Technical Specification of Wired Section of the Solution			
S/No.	Specifications	YES/NO	Remarks
1.	All the proposed switches must be manageable, of enterprise class (not small business) and of Cisco/Juniper/Extreme make only, with full-fledged Layer-2 functionality. Switches must be accessible via SSH/Telnet.		
2.	All Switches listed under S/No 2 and 3 of the attached BOQ must have 1G SFP ports with 10Gbps SFP+ uplink. The switch must have redundant power supply.		
3.	All Switches listed under S/No 4 and 5 of the attached BOQ must have 10/100/1000 Mbps UTP ports with 1Gbps SFP uplink.		
4.	All SFP+ and SFP transceivers listed under S/No 6 and 7 of the attached BOQ must be of the same make as the quoted Switches.		
5.	All interconnections between Switches must be via Single Mode Optical Fiber (OFC) (9/125µm) except for cases where up-link and down-link switches are housed in the same Network rack.		
6.	All passive components of the wired network for the project listed under S/No. 8 to 21 in the attached BOQ must be of COMMSCOPE/TYCO/SYSTIMAX/BELDEN make only.		
7.	All network racks listed under S/No 22 and 23 of the attached BOQ must be of Netrack/Valrack/Rittal make only.		
8.	All PVC ducts listed under S/No. 24 to 26 in the attached BOQ must be of LEGRAND/MODI/MK make only.		
9.	All outdoor OFC cabling must be routed via HDPE pipes of PE-63 or higher which must be at least 1.5 inches in diameter and bearing ISI marking that must be buried underground at least 3 feet deep from solid surface.		
10.	All indoor OFC cabling must be routed in PVC conduit bearing ISI marking as listed under S/No. 26 in the attached BOQ.		

11.	All indoor Cat 6 UTP cabling must be routed in PVC casing and capping with ISI marking as listed under S/No. 24 and 25 in the attached BOQ with numbered ferrule at both ends.		
12.	All electrical components listed under S/No. 31 and 32 in the attached BOQ must be of LEGRAND/BELKIN/GM make only.		
13.	All indoor electrical cabling must be routed in the same PVC conduit along with OFC as mentioned in the item 1.8 above.		
14.	All UPS listed under S/No. 28 to 30 in the attached BOQ must be of APC/EMMERSON make only.		
15.	All Batteries listed under S/No. 28 to 30 in the attached BOQ must be of AMARON/EXIDE make only.		
16.	All Power Cords used to connect to all active devices must be 3-pin, round pin 5/15 AMP Power Cord.		
17.	All UTP cabling must be labelled on both Jack Panel end and Access Point end. The label must have information about Floor Number, Information Outlet number, Access point location (room number where AP is installed).		
18.	All OFC cabling must be labelled on both LIU ends. The label must have information of both Uplink and Downlink location, Floor number and room number.		
19.	All visible cables and patch cords must be neatly dressed and a routed in an orderly manner.		
20.	All road crossings must be via horizontal directional drilling (HDD).		

Technical Specification of Wi-Fi and WIPS of the Solution

S/No.		YES/NO	REMARK
21.	The proposed Controller and Access Points must be of Cisco/HPE(Aruba)/Arista make only.		
22.	The Wi-Fi Access Points should have a total of 3 or more radios, of which at least two should be dedicated 2x2 MU-MIMO radios for Wi-Fi access on both 2.4 GHz and 5 GHz bands, and at least one dedicated radio for WIPS and automatic channel		

	allocation, operating simultaneously in a single device.		
23.	The solution must support wireless intrusion prevention system (WIPS) without effecting Wi-Fi performance.		
24.	Apart from DC power, the Wi-Fi Access Points and WIPS must work with all features supported on 802.3at PoE+.		
25.	Wi-Fi Access Points and the solution must support the following protocols: IEEE 802.11a/b/g, IEEE 802.11n, IEEE 802.11ac (WAVE 2), IEEE 802.11h, IEEE 802.11d, 802.11i.		
26.	The Wi-Fi Access Points devices and the solution should support the following authentication methods: 802.1X support, per-session encryption keys (WPA2).		
27.	Wi-Fi Access Points and WIPS should be remotely upgradeable from the controller, so that new features / upgrades can be added.		
28.	Wi-Fi Access Points should be approved by the Wireless Planning Commission (WPC).		
29.	Wi-Fi Access Points should have two-way band steering (example from 2.4GHz band to 5GHz and from 5 GHz to 2.4 GHz).		
30.	Wi-Fi Access Points should facilitate auto channel allocation to avoid interference between APs.		
31.	Wi-Fi Access Points and the solution should support configuration in both Bridge and NAT modes.		
32.	Wi-Fi Access Points and the solution should support 802.1Q VLANs. Further it should be possible to set Trunk Ports on Access Points.		
33.	Wi-Fi Access Points should support configurable management VLAN (support other than VLAN-1 as management VLAN).		
34.	Wi-Fi Access Points should be ceiling mountable.		
35.	Supply should include as many ceiling mountable units as the number of Access Points quoted.		
Architecture of WLAN and WIPS			
S/No.		**YES/NO**	**REMARK**

36.	Proposed Wi-Fi management solution shall be a scalable cloud based for central management of all Wi-Fi/WIPS functionality. Further, it should support remote replication w.r.t DR.		
37.	Solution must support intelligent edge architecture for Wi-Fi access and wireless intrusion prevention (WIPS). All WLAN services should be delivered at the edge, eliminating the dependency on the controller i.e. all Wi-Fi & WIPS services should be functional on the device even if the link between AP and its management controller or the controller itself goes down.		
38.	The solution must facilitate Control and Provisioning of Wireless Access Point devices and ensure data encryption between access point devices and controllers across WAN/LAN links.		
39.	Wi-Fi controller should support deployment of set policies across the Wi-Fi AP devices placed on different network segments over LAN and WAN.		
40.	The Controller and Access Point device should support dual stack for IPV4 and IPV6.		
41.	Wireless manager solution must be PCI DSS and FIPS140-2 certified.		
42.	The solution should be able to work in a heterogenous environment by not hindering the operation of existing APs of different makes already deployed at IISc.		
Wi-Fi Management			
S/No.		**YES/NO**	**REMARK**
43.	The Wi-Fi management controller should be cloud based with High Availability.		
44.	The solution must provide centralized Wi-Fi and WIPS management of the entire solution for both Wi-Fi and WIPS.		
45.	Quote should include all required Hardware and Software licenses to support all the Access Points and WIPS as listed under S/No. 1 of the attached BOQ. There should not be any additional licenses required for DR.		
46.	The solution must be scalable to support up to 2000 Access points and WIPS.		

47.	The solution must be able to simultaneously broadcast multiple SSIDs (at least 4) as visible network to client.		
48.	The solution should have the ability to create customizable dashboards.		
49.	The solution should have all-locations-consolidated dashboard and location-specific dashboard as well.		
50.	Solution should have role-based admin rights.		
51.	The solution must have policy-based management and administration.		
52.	The solution should detect and identify all types of Wi-Fi enabled client devices.		
53.	The solution must provide forensic data aggregated for major threat vectors like Rogue AP, Honeypot AP, Mis-Configured AP, DoS, Unauthorized Association, Ad Hoc Networks, Bridging/ICS Client, Mis-Association.		
54.	The solution should provide real-time RF coverage maps for the managed APs to help estimate RF coverage and leakage.		
55.	The solution should locate wireless devices (APs and Clients) accurately on floor maps.		
56.	The solution must provide location tracking of a DoS attacker.		
57.	Both the controller and Wi-Fi device should support SNMP v2c, v3.		
58.	The solution should support Captive Portal.		
59.	The solution should support External Splash Page.		
60.	The solution should support RADIUS, Active Directory and LDAP based authentication for both Corporate as well as Guest Clients.		
61.	The solution should support “Walled Garden” or equivalent feature for Guest Network.		
62.	The solution should support URL redirection.		
63.	The solution should provide Guest Client association time-out.		
64.	Solution should allow blocking of Guest user for specific time frame between two active sessions.		

65.	The solution should provide remote packet capture for troubleshooting.		
66.	The solution should support manual and automatic scheduling of system backup.		
67.	The solution should maintain logs which includes all activities performed by the users like login, any configuration changes made on the system, device deletion, device authorization, log out etc., for at least 365 days.		
68.	The solution should enable wireless client association analytics logs that includes client MAC address, AP connected to, data transfer, data rate, session duration, content - domain (http, https, IP address), for at least 180 days.		
69.	The solution should support uploading of all logs to external Syslog Server in LAN/WAN on real-time and scheduled basis.		
70.	The solution should provide application visibility. It should display list of applications with their data usage for a given SSID.		
71.	The solution should block traffic based on IP address, port, URL, hostname etc. and QoS (for example: bandwidth restriction for the SSID, QoS tagging of special traffic like Voice) at the edge (AP).		
72.	The solution must allow VLAN segmentation at the edge.		
73.	The solution must support Advanced Encryption Standards (AES), Temporal Key Integrity Protocol (TKIP).		
74.	Time Schedules - the solution must allow configuration of time schedules when WLAN is / is not available for a single or group of APs (For example: SSIDs can be active from 9 am to 5 pm and then automatically disabled and enabled).		
75.	The threat detection in the solution must be based on behavioural model (resilience against Zero-day attacks), in addition to signature based and threshold tuning.		
76.	The solution must have the capability of auto classifying Wi-Fi clients as authorized (managed clients connecting to IISc, Bangalore network), guest, rogue (un-managed client attempting		

	connection to IISc, Bangalore network) or external (unmanaged not connecting to IISc, Bangalore network e.g. neighbour), in addition to manual classification.		
77.	The solution must indicate if it cannot reliably detect connectivity of Access Points.		
78.	The solution must be able to detect all types of Rogue (unauthorized APs connected to IISc, Bangalore network) Access Points.		
79.	The solution must detect mis-configured authorized Access Points.		
80.	The solution should be able to detect and prevent (if configured to do so) outside client trying to connect to the IISc, Bangalore network.		
81.	The solution should be able to detect and prevent (if configured to do so) all types of Ad-Hoc connections.		
82.	The solution must detect Honey Pot attacks including its advanced variants such as Multipot.		
83.	The WIPS solution should not affect the operation of other Access Points while preventing a rogue AP on the same channel.		
84.	The solution must be able to detect wireless Denial of Service (DoS) attacks.		
85.	Wi-Fi controllers License should work across subnets to reach Wi-Fi Access Points deployed in various network segments.		
86.	Wi-Fi controllers should support enforcing policies across multiple Access Points.		
87.	Wi-Fi controller should support both active / active and active / passive modes of operation.		
Management and Monitoring			
S/No.		**YES/NO**	**REMARK**
88.	The solution should provide alerts in hierarchical structure.		
89.	The solution must send notifications based on location and alarm type.		
90.	The solution must support addition of tags and notes to devices.		
91.	The solution must provide a device summary (for APs and clients) report per location.		

92.	The solution must allow customization of existing reports and creation of new reports by an administrator.		
93.	The solution must allow automatic schedules for report generation and distribution of reports to specific users. • High number of client association • High number of client association • Excessive frame re-transmission • Low average data rate for a client • Drop in a signal of an Access Point • Inadequate coverage		
94.	The solution should have built-in, make & model agnostic performance monitoring and Wi-Fi Analytics.		
95.	The controller and Wi-Fi AP devices management should support command line (SSH / telnet and as well as web based (HTTPS) administration.		
	Guest Management		
S/No		**YES/NO**	**REMARK**
96.	Solution should allow enabling/disabling guest login features.		
97.	Solution should support multiple authentication mechanisms to authenticate guest users through a single captive portal, with an option of using any one or a combination (e.g.: Username and Password and/or SMS OTP) of authentication mechanisms.		
98.	Guest user should be able to authenticate with the Wi-Fi using a self-registration process, where the user will enter some requested information and an authorized person will check and approve the request and Wi-Fi access should be granted automatically post approval. For example: Solutions should support guest user authentication by SMS, social media, self-registration, where an authorized user can provide access to a guest after email verification.		
99.	The solution should support integration with SMTP server to send Wi-Fi access details via e-mail to guest users.		

100.	The solution should provide location-aware visitor, usage, loyalty, and social analytics information through different graphs of guest users.		
101.	The solution should provide the graphs that represent the data received, transmitted & total data exchange by days and location of guest users.		
102.	The solution should also provide various guest user management functions, such as importing and exporting guest user accounts and enabling and disabling guest user accounts.		
103.	The solution should be able to maintain profiles of the users connected to the guest Wi-Fi network; profiles should provide information such as login location, first name, last name, mobile number, last authentication time, email etc.		
Coverage and Capacity Planning			
S/No		**YES/NO**	**REMARK**
104.	On-site site survey by the bidder is required to plan Wi-Fi deployment in each floor of each building.		
105.	The solution must ensure at least -65 dBm RSSI inside all hostel rooms.		
106.	The bidder should provide the location of Access Points on the floor plan for all buildings (Note: tentative location plan will be provided by IISc).		
107.	The bidder should provide OEM-certified coverage heat map for 2.4 GHz and 5 GHz separately with - 65 dBm RSSI threshold for 2.4 GHz. All coverage holes in the premises should be indicated clearly.		
108.	The bidder should provide OEM-certified AP coverage redundancy map.		
License, Warranty and Support:			
S/No		**YES/NO**	**REMARK**
109.	The total solution should include licenses for all necessary features from the first day of the installation. All the licenses quoted should be perpetual. All the features and signatures including WIPS available at the time of expiration of license should continue to work. Renewal of licenses should be required only for new features and updates/releases announced by the OEM after the contract expires.		

110.	The total solution should have 3 years’ on-site warranty for Access Points, Switches, UPS & batteries, cabling & accessories, and cloud-based controller subscription.		
111.	The total solution should include technical support for software/firmware and software upgrades for controller, Access Points and Switches for 3 years.		
112.	The total solution should be upgradable to the latest stable version, as and when available, at no extra cost.		
113.	The quote should also include additional 2 years’ AMC specified as a separate line item.		
114.	Warranty support should include 4 hrs. response time and provision of replacement along with appropriate configuration and installation in next business day for Hardware.		
115.	Should provide single point of contact and should provide call logging and escalation matrix.		

ANNEXURE-3 (BOQ)

Supply

S/No	Particulars	Quantity	Units
1	Wi-Fi Access Point with at least 3 radios, of which at least 2 must be 2x2 MU-MIMO broadcasting at 2.4Ghz and 5Ghz and at least 1 dedicated for WIPS and automatic channel allocation with cloud based controller in HA mode.	1000	Nos
2	24 SFP ports with 2 SFP+ ports layer-2 manageable 1G/10G switch with dual power supply	4	Nos
3	12 SFP ports with 2 SFP+ ports layer-2 manageable 1G/10G switch with dual power supply	6	Nos
4	24 UTP port POE+ switch with 4 SFP port layer-2, 10/100/1000 Mbps manageable switch having at least 375 W power budget for POE (Support POE+ on 12 ports concurrently)	13	Nos
5	24 UTP port POE+ switch with 2 SFP port layer-2, 10/100/1000 Mbps manageable switch having at least 375 W power budget for POE (Support POE+ on 12 ports concurrently)	152	Nos
6	Single Mode 1310 nm SFP+ transceiver (10GBASE-LR)	20	Nos
7	Single Mode 1310 nm SFP transceiver (1000BASE-LX)	330	Nos
8	6-Core Single Mode (9/125µm) armoured outdoor Optical Fibre Cable in meters	5000	Meters
9	4-Core Single Mode (9/125µm) indoor Optical Fibre Cables in meters	24000	Meters
10	CAT 6 UTP cable in meters	42000	Meters
11	Unloaded UTP Jack Panel	165	Nos
12	CAT 6 Information Outlet compatible with jack panel mentioned above	1000	Nos
13	RJ45 connector	1000	Nos
14	24 fibre core LIU with LC connector, mountable in 19’’ network rack	26	Nos
15	12 fibre core LIU with LC connector, mountable in 19’’ network rack	7	Nos
16	6 Fibre Core LIU with LC connector, mountable in 19’’ network rack	21	Nos
17	Cable manager mountable in 19” Network Rack	219	Nos
18	CAT 6 UTP Patch Cord 1 meter	1000	Nos
19	Single Mode pigtail with LC connector	1500	Nos
20	LC-LC single mode duplex patch cord 2 meters	175	Nos
21	LC-LC single mode duplex patch cord 1 meter	160	Nos
22	19 inch, 530 mm depth, 9U Wall Mountable Network rack with 4 socket power strip	165	Nos

23	19 inch, 1000 mm depth, 32U Floor Standing Network rack with 8 socket power strip	9	Nos
24	PVC casing and capping 25x25mm in meters with necessary accessories	25000	Meters
25	PVC casing and capping 45x45mm in meters with necessary accessories	4200	Meters
26	PVC conduit of diameter of 32mm in meters with necessary accessories	19000	Meters
27	1.5 inch HDPE pipe with of PE-63 or higher in meters	1500	Meters
28	20 KVA, 3φ input 3φ output online UPS with 1200AH SMF Batteries with necessary accessories	4	Nos
29	5 KVA, 1φ online UPS with 360AH SMF Batteries with necessary accessories	7	Nos
30	3 KVA, 1φ online UPS with 180AH SMF Batteries with necessary accessories	12	Nos
31	5/15 AMPS round pin power socket with switch and back box	175	Nos
32	3 core, 1.5 sq mm wire, shielded copper electrical cable in meters	20000	Meters
33	Ceiling mountable extension pole with 45° angle bracket of Metal MS/Aluminium with powder coating for mounting Access Point	100	Nos

Services

S/No	Particulars	Quantity	Units
34	Configuration and Installation/mounting on celling or angle bracket of Access points with labelling	1000	Nos
35	Configuration and Installation of Network Switches in network rack with labelling	175	Nos
36	Excavation of soil (depth 3 feet, width 1 feet) and resurfacing for burial of HDPE Pipe per running meter	3000	Meters
37	Excavation of soil and construction of 3x3x3 ft brick chamber with RCC lid for pulling outdoor OFC	20	Nos
38	Horizontal Directional Drilling (HDD) for crossing roads in meters	800	Meters
39	Installation of UTP cables through PVC casing and capping in meters	42000	Meters
40	Installation of indoor OFC through PVC conduit in meters	24000	Meters
41	Installation of indoor electrical cables through PVC conduit in meters	20000	Meters
42	Installation of PVC conduit in meters	48200	Meters
43	RCC core cutting of 3 inch diameter for inter-floor wiring	20	Nos
44	Installation of HDPE pipe underground (3 feet from solid surface) in meters	1500	Meters

45	**Installation of outdoor OFC through HDPE pipe in meters**	5000	Meters
46	**Installation, termination and labelling of UTP cables on Jack Panel**	1000	Nos
47	**Termination and labelling of UTP cables on RJ45 Connector**	1000	Nos
48	**Installation and labelling of LIU**	54	Nos
49	**Fusion splicing of pigtails with OFC inside LIU**	1500	Nos
50	**Installation of power socket**	175	Nos
51	**Installation of 32U network rack with cable dressing and labelling on patch cord**	9	Nos
52	**Installation of 9U network rack with cable dressing and labelling on patch cord**	165	Nos
53	**Installation of 20KVA UPS and batteries with proper earthing and MCB**	4	Nos
54	**Installation of 5KVA UPS and batteries with proper earthing and MCB**	7	Nos
55	**Installation of 3KVA UPS and batteries with proper earthing and MCB**	12	Nos
56	**Documentation of the entire project as mentioned in RFP**	1	Nos
57	**Testing and generating reports as mentioned in RFP**	1	Nos
58	**AMC charges for addition 2 years post 3 years warranty**	1	Nos

ANNEXURE-4 (BOQ Compliance Sheet)

Supply

S/No	Particulars	Quantity	Units	Included in the commercial bid (YES/N0)	Remark
1	Wi-Fi Access Point with at least 3 radios, of which at least 2 must be 2x2 MU-MIMO broadcasting at 2.4Ghz and 5Ghz and at least 1 dedicated for WIPS and automatic channel allocation with cloud based controller in HA mode.	1000	Nos		
2	24 SFP ports with 2 SFP+ ports layer-2 manageable 1G/10G switch with dual power supply	4	Nos		
3	12 SFP ports with 2 SFP+ ports layer-2 manageable 1G/10G switch with dual power supply	6	Nos		
4	24 UTP port POE+ switch with 4 SFP port layer-2, 10/100/1000 Mbps manageable switch having at least 375 W power budget for POE (Support POE+ on 12 ports concurrently)	13	Nos		
5	24 UTP port POE+ switch with 2 SFP port layer-2, 10/100/1000 Mbps manageable switch having at least 375 W power budget for POE (Support POE+ on 12 ports concurrently)	152	Nos		
6	Single Mode 1310 nm SFP+ transceiver (10GBASE-LR)	20	Nos		
7	Single Mode 1310 nm SFP transceiver (1000BASE-LX)	330	Nos		
8	6-Core Single Mode (9/125µm) armored outdoor Optical Fiber Cable in meters	5000	Meters		
9	4-Core Single Mode (9/125µm) indoor Optical Fiber Cables in meters	24000	Meters		
10	CAT 6 UTP cable in meters	42000	Meters		
11	Unloaded UTP Jack Panel	165	Nos		
12	CAT 6 Information Outlet compatible with jack panel mentioned above	1000	Nos		

13	RJ45 connector	1000	Nos		
14	24 Fibre core LIU with LC connector, mountable in 19’’ network rack	26	Nos		
15	12 Fibre core LIU with LC connector, mountable in 19’’ network rack	7	Nos		
16	6 Fibre Core LIU with LC connector, mountable in 19’’ network rack	21	Nos		
17	Cable manager mountable in 19” Network Rack	219	Nos		
18	CAT 6 UTP Patch Cord 1 meter	1000	Nos		
19	Single Mode pigtail with LC connector	1500	Nos		
20	LC-LC single mode duplex patch cord 2 meters	175	Nos		
21	LC-LC single mode duplex patch cord 1 meter	160	Nos		
22	19 inch, 530 mm depth, 9U Wall Mountable Network rack with 4 socket power strip	165	Nos		
23	19 inch, 1000 mm depth, 32U Floor Standing Network rack with 8 socket power strip	9	Nos		
24	PVC casing and capping 25x25mm in meters with necessary accessories	25000	Meters		
25	PVC casing and capping 45x45mm in meters with necessary accessories	4200	Meters		
26	PVC conduit of diameter of 32mm in meters with necessary accessories	19000	Meters		
27	1.5 inch HDPE pipe with of PE-63 or higher in meters	1500	Meters		
28	20 KVA, 3ϕ input 3ϕ output online UPS with 1200AH SMF Batteries with necessary accessories	4	Nos		
29	5 KVA, 1ϕ online UPS with 360AH SMF Batteries with necessary accessories	7	Nos		
30	3 KVA, 1ϕ online UPS with 180AH SMF Batteries with necessary accessories	12	Nos		
31	5/15 AMPS round pin power socket with switch and back box	175	Nos		
32	3 core, 1.5 sq mm wire, shielded copper electrical cable in meters	20000	Meters		
33	Ceiling mountable extension pole with 45° angle bracket of Metal MS/Aluminum with powder coating for mounting Access Point	100	Nos		

Services

S/No	Particulars	Quantity	Units	Included in the commercial bid (YES/N0)	Remark
34	Configuration and Installation/mounting on ceilng or angle bracket of Access points with labelling	1000	Nos		
35	Configuration and Installation of Network Switches in network rack with labelling	175	Nos		
36	Excavation of soil (depth 3 feet, width 1 feet) and resurfacing for burial of HDPE Pipe per running meter	3000	Meters		
37	Excavation of soil and construction of 3x3x3 ft brick chamber with RCC lid for pulling outdoor OFC	20	Nos		
38	Horizontal Directional Drilling (HDD) for crossing roads in meters	800	Meters		
39	Installation of UTP cables through PVC casing and capping in meters	42000	Meters		
40	Installation of indoor OFC through PVC conduit in meters	24000	Meters		
41	Installation of indoor electrical cables through PVC conduit in meters	20000	Meters		
42	Installation of PVC conduit in meters	48200	Meters		
43	RCC core cutting of 3inch diameter for inter-floor wiring	20	Nos		
44	Installation of HDPE pipe underground (3 feet from solid surface) in meters	1500	Meters		
45	Installation of outdoor OFC through HDPE pipe in meters	5000	Meters		
46	Installation, termination and labelling of UTP cables on Jack Panel	1000	Nos		
47	Termination and labelling of UTP cables on RJ45 Connector	1000	Nos		
48	Installation and labelling of LIU	54	Nos		
49	Fusion splicing of pigtails with OFC inside LIU	1500	Nos		
50	Installation of power socket	175	Nos		
51	Installation of 32U network rack with cable dressing and labelling on patch cord	9	Nos		
52	Installation of 9U network rack with cable dressing and labelling on patch cord	165	Nos		

53	**Installation of 20KVA UPS and batteries with proper earthing and MCB**	4	Nos		
54	**Installation of 5KVA UPS and batteries with proper earthing and MCB**	7	Nos		
55	**Installation of 3KVA UPS and batteries with proper earthing and MCB**	12	Nos		
56	**Documentation of the entire project as mentioned in RFP**	1	Nos		
57	**Testing and generating reports as mentioned in RFP**	1	Nos		
58	**AMC charges for addition 2 years post 3 years warranty**	1	Nos		

ANNEXURE 5

Details of the Bank Account of IISc Bangalore for submitting EMD / Bid Security / Performance Security / Security Deposit

Account's Name: **I.I.Sc.**

Bank: **State Bank India**

Branch: **IIS Bangalore**

Branch Code: **02215**

Account No.: **31728098170**

IFSC: **SBIN0002215**

MICR: **560002020**

Note:

- It is mandatory to write Name & Address of the Bidder and Tender Reference No. & Date on the back side of the e-receipt of NEFT/RTGS.
- Acceptance of the e-receipt of NEFT/RTGS is subject to its verification from Finance & Accounts section.

ANNEXURE 6

FORMAT FOR BANK GUARANTEE FOR PERFORMANCE SECURITY (PERFORMANCE BANK GUARANTEE)

To
The Registrar
Indian Institute of Science (I.I.Sc.)
Bangalore – 560 012 (Karnataka, India)

Subject: Performance Bank Guarantee (PBG)

Reference: I.I.Sc. Purchase Order No. ________________________________ dated ___________

Dear Sir,

1. We hereby issue a Bank Guarantee as follows: -

   Bank Guarantee No. ________________________ Date: ___________
   Amount of Guarantee Rs. ___________,
   Guarantee covers From _________________ To ______________
   Last Date for Lodgement of Claim: _________________

2. This deed of Guarantee executed by the (Name of the Bank: _________________) constituted under _______________________ Act, ______ having its Central Office at ____ and amongst other places a branch at ____ (hereinafter referred to as "The Bank") in favour of The Registrar, Indian Institute of Science, Bangalore – 560 012 (hereinafter referred to as I.I.Sc.) for an amount of not exceeding Rs. ___________ (in words: Rupees.____ only) at the request of M/s _____________________________________(hereinafter referred to as the "Contractor" / "Supplier").

3. In consideration of The Registrar, Indian Institute of Science, Bangalore – 560 012 (hereinafter called I.I.Sc.) having entered into an agreement vide IISc's Purchase Order No. __________________________dated_________ with M/s _____________________ (hereinafter called the Supplier) to carry out the supply and installation of the ____ __<Name of the equipments/work/Job> at Indian Institute of Science, Bangalore as per their above order, the Supplier agreed to execute a Bank Guarantee for 10% of the total order value viz. Rs. ___________ (Rupees ____) towards Performance Security / Performance Guarantee obligation for a period of ___ year(s) / mo nth(s) from ______________ to ____________.

4. We, the ____________________ Bank, __________________Branch (hereinafter referred to as a Guarantor) at the request of the supplier, irrevocably undertake to indemnify and to keep indemnify I.I.Sc. without any demur to the extent of Rs.____________ (Rupees _______________________________________) in the event of the aforesaid Supplier failing to comply the Warranty / contractual Obligations as per the agreed terms to the full satisfaction of the Company as mentioned in the I.I.Sc.'s purchase order.

5. NOW THIS BANK HEREBY GUARANTEES that in the event of the said Supplier failing to abide by any of the conditions referred in tender document / purchase order / performance of the equipment / Machinery / service, etc. this Bank shall pay to Indian Institute of Science, Bangalore on demand and without protest or demur Rs .... (Rupees....................................).

6. We __________________Bank, further agree that the Guarantee herein contained shall remain in full force and affect during the period that would be taken for the performance of the equipment and / or services as stated in the Purchase Order issued by I.I.Sc. and that it shall continue to be enforceable till the completion of the period and certified that warranty and contractual obligations have been fully carried out by the supplier and accordingly discharges the Guarantee subject. However, I.I.Sc. shall have no right under after the expiry of the Guarantee, i.e. ___________(date).

7. We, _______________________Bank undertake not to revoke this Guarantee, during its currency except with the previous consent of I.I.Sc. in writing.

8. Notwithstanding anything contained herein,
   (a) Our liability under the Bank Guarantee shall not exceed Rs.____________ (Rupees ____).
   (b) This Bank Guarantee shall be valid up to _______________.
   (c) We are liable to pay the guaranteed amount or any part thereof under this Bank Guarantee only and only if I.I.Sc. serve upon us a written claim or demand on or before expiry of date (i.e.___________).

9. NOTWITHSTANDING anything contained herein above, our liability under this Guarantee is restricted to Rs. ____________ (Rupees ____only) our guarantee shall remain in force until. Unless a Demand or claim under the guarantee is made on our Bank in writing on or before _____________ all your rights under the said guarantee be forfeited and we shall be relieved and discharged from all liabilities thereunder.

10. This Bank further agrees that the decision of Indian Institute of Science, Bangalore as to whether the said Supplier has committed a breach of any of the conditions referred in tender document / purchase order shall be final and binding.

11. This Bank further agrees that the claims if any, against this Bank Guarantee shall be enforceable at our branch office at .... situated at .... (Address of local branch) as following details:

Name of the Bank	
Branch Name	
Branch Code	
IFSC Code	
E-mail Id	
Phone / Mobile No.	

Seal & Signature of the Bank