EOI/ RFP invited from
Central Govt./ State Govt. Public Sector Undertakings (PSU)
For implementation of LAN and Wi-Fi Campus
in Sambalpur University.

Contents

1. Objective:

Sambalpur University is one of the leading State University in the Western Odisha intend to establish Campus Wi-Fi LAN to meet the need of providing seamless internet and intranet access across Univ. Campus. The proposed Campus Wi-Fi LAN would not only improve the overall educational experience but will also support the institution's operational and administrative needs. This bid is limited to participation from Central Govt. /State Govt. Public Sector Undertakings only who qualifies the Bidder's eligibility criteria. The Key Objective and benefits we intend to achieve are listed as below:

I. Enhanced Accessibility
   - **Enable Widespread Coverage:** which will allow students, faculty, and staff to access the internet from various locations within the campus.
   - **Mobility:** Facilitates learning and collaboration from different areas, such as libraries, dorms, and outdoor spaces.

II. Improved Learning and Teaching
   - **Access to Online Resources:** ensure to Provide easy access to educational materials, research databases, and e-learning platforms.
   - **Interactive Learning:** to Support the use of digital tools and applications for interactive and multimedia-rich teaching methods.

III. Facilitated Communication
   - **Ensure Seamless Connectivity:** Build a network which Enhances communication through email, messaging apps, and video conferencing, making it easier for students and staff to stay connected.
   - **Provision Collaboration Tools:** to Support the use of collaborative platforms and futuristic cloud services for group projects and academic discussions.

IV. Increase Operational Efficiency
   - **Administrative Functions:** Create backbone for enablement of Streamlining administrative processes, such as enrolment, scheduling, and grading etc., through online systems.

- **Resource Management:** Build a campus-wide effective management of campus resources, including library catalogues, student information systems, and digital signage.

V. Student Engagement and Retention

- **Modernizing & Engaging Learning Environment:** Create a more engaging and modern learning environment that can enhance student satisfaction and retention.
- **Access to Services:** Build network for provisioning access to online student services, including virtual help desks, counselling, and academic support.

VI. Cost-Effective Network

- **Reduction in Infrastructure Costs:** which Minimizes the need for extensive wired infrastructure, which can be costly to install and maintain.
- **Scalability:** establish a network that is easily scalable to accommodate increasing numbers of users or changes in technology needs in the future.

VII. Ensure Enhanced Network & Cyber Security

- **Network Management:** the proposed network must guarantee centralized management of network security, including monitoring and access control.
- **Data Protection:** the aimed network must provide options for implementing security protocols to protect sensitive information and prevent unauthorized access.

2. Scope of Work/ Supply

I. **Establishment of Secure Campus wide Wi-Fi and LAN at 80 locations in Sambalpur University Campus, Sambalpur, Odisha as per attached list of locations – Annexure 1**

II. Go-live of the project will commence from the date of supply, installation and commissioning of equipment's across the Campus. Any site which will not be ready for deployment – a written note along with site photographs must be submitted to the competent authority of university.

III. The bidder will ensure timely delivery of all equipment's at site

IV. The bidder will get all material checked by the competent authority in terms of quantity, model, make.

V. The bidder will be responsible for smooth functioning of Campus Wi-Fi network, availability of spares, trained staff, training of the university staff.

VI. Bidder will maintain at least one Resident Engineer to deliver the SLA 95% and will ensure managing and timely upgradation of all patches, software updates in all devices being installed in the Campus.

VII. Bidder Implementation team will prepare HLD (High Level design) of the proposed Campus Wi-Fi & LAN and get the same approved by the competent authority before they start the deployment. The bidder will maintain all configuration details in both hard Copy and Soft Copy, CAD Drawing of the established Campus Network, Laminated Network design on at least A0 Size properly framed, Final LLD (Low-Level Design) with details basis component level and connectivity type and route.

VIII. Bidder needs to utilize all the functionality of installed gateway NGFW firewall to ensure the already designed and implemented security policies are not compromised.

IX. Competent authority will ensure receipt of all items being supplied by the bidder as per the Work order in good condition and provisioned proper secure & storage space – which will have locking facility with no Seepage, electricity etc. the bidder has to arrange the locking and safety of material.

X. University will provision proper 3-Phase RAW Power 24x7 at all locations and Chemical earthing must be done and maintained by the bidder during the contract period. Source of power must be provided at the devices RACK installation. Any deficiency in SLA due to non-availability of Power, Internet bandwidth will not be credited to the account of bidders'.

XI. University must have provision for electrical wiring from electrical Panel/distribution box up to Network RACKS being installed at various locations in the Campus. The type and core of electrical cable, type of Socket will be provisioned by the bidders in HLD.

XII. University shall provide the availability of proper storage of material, sitting space for the bidder team, proper lockable room for keeping tools and spares.

XIII. University shall provide two rooms in the Campus Guest House for the period of project execution & implementation.

XIV. The competent authority will grant permissions to lay cables, dig roads (if necessary), space for installing RACKS, permission to work 24x7, Saturday & Sunday, Holidays, if necessary to ensure the timely completion of the work.

XV. The scope involves digging and laying of fibre/copper cable in duct thru HDD/ moiling/ open process as per CPWD/ PWD standards and refurbish the site in original condition.

XVI. The scope involves constructing/ supply and installation of pole mounting structure, main holes for fibre laying with OFC route marker etc.

XVII. The scope also involves supply, laying/ drawing, termination of minor electrical work which include cable, conduit etc. to power up the equipment/ accessories from the nearest power source as advised by the buyer.

XVIII. Supply and mounting of UPS with rack and 60 Minutes of power backup shall be also in bidder scope. The bidder must do the power calculation, their own before quoting in the bid.

XIX. As this is a BoQ based bid, the billing shall be done as per actual consumption basis, which should be duly certified by the competent authority.

3. Campus Wi-Fi LAN expected functionalities

We chose to build the Campus Wi-Fi and secure LAN infrastructure which would provide a comprehensive and flexible framework for deploying secure communication medium and moreover ensuring that it meets the needs of the institution while allowing for future expansion and technological advancements in the field of networking and internet access.

The technical proposal shall contain network topology, schematic diagram of backbone, schematic diagram of OFC ring and building wise bill of material. The datasheet /technical specifications along with make and model of networking hardware/equipment/items should be mentioned in the technical proposal.

The prospective bidder must ensure the below functionality which should be completely considered while ensuring Supply, Planning & Implementation of the Campus Wi-Fi and LAN.

1. **Scalability:** Ensure that the network design can accommodate future growth in users and devices.
2. **Redundancy and Fault Tolerance:** Implement redundant paths and failover mechanisms to maintain network reliability.

3. **Security:** Employ robust security measures to protect sensitive data and prevent unauthorized access.
4. **User Experience:** Optimize the placement of access points and configure the network to provide high-speed, reliable connectivity.
5. **Performance and Scalability**
    a. **Traffic Management:** Campuses often experience high traffic volumes, especially during peak hours. A well-designed network architecture must be proposed to ensure efficient traffic management, preventing congestion and maintaining optimal performance.
    b. **Load Balancing:** Proper architecture design & policies must be proposed to allow for load balancing across multiple access points and network devices, ensuring that no single device becomes a bottleneck.
    c. Must be a scalable network design which allows for easy expansion without significant redesign or disruptions.
    d. The proposed design must be flexible and Modular architecture which enables the addition of new features or technologies as needed, accommodating evolving needs of the university.
6. **Coverage and Connectivity**
    a. The campus must have adequate Wi-Fi coverage, minimizing dead zones and providing reliable connectivity
    b. The network design proposed must be centrally managed and designed to mitigate interference from physical obstacles or other wireless devices and maintaining connectivity and performance.
    c. Seamless Roaming: A well-architected network must be proposed, designed to ensure seamless handoff between access points, ensuring that users experience uninterrupted connectivity as they move around the campus.
7. **Operational Efficiency**
    a. **Centralized Management:** Bidders proposed Network architecture should facilitate centralized management and monitoring, making it easier for University IT staff to configure, maintain, and troubleshoot the network.
    b. Integration of automated tools for configuration management, monitoring, and updates can streamline operations and reduce administrative overhead.

c. Monitoring tool must Perform synthetic testing from multiple vantage points to monitor application uptime, user experience, and performance
d. Must ensure Improved customer and end-user experience by proactively identifying service degradation
e. Must Correlates network and application performance data to quickly pinpoint root cause of issues
f. Implementing a dual ring (a backup ring) to provide the redundancy. If one ring fails, the network can continue operating on the secondary ring, ensuring higher reliability.
g. Built Fault Isolation - If one cable or device fails, it typically doesn't affect the rest of the network. This isolation helps maintain overall network stability.
h. All the Ethernet switches must be natively integrated with existing Perimeter gateway Security device using management interface, allowing for centralized control of both security and networking components. This integration should ensure simplified network management by providing a single pane of glass for configuration, monitoring, and troubleshooting.
i. We should be able to manage all switches and firewalls through a single interface, apply consistent security policies across the network, should be able to leverage information from switches to detect and respond to threats more effectively.
j. Enable segmentation to improve security by isolating different network segments and controlling traffic between them
k. No manual intervention the proposed design/technology must have zero-touch provisioning, allowing for automatic configuration of switches etc. when they are added to the network.

8. **User Experience**
    a. The proposed Effective network architecture must support Quality of Service (QoS) features that prioritize critical applications and services, ensuring a consistent and high-quality user experience.
    b. The proposed network design must be proper, which reduces latency and ensures fast response times for applications and services.

9. **Preventing Unauthorized Access**
    a. The bidder proposed Network Architecture must ensure proper security measures, restrict unauthorized users any access to the network, which might potentially lead to data theft, vandalism, or misuse of resources.
    b. Guest user policy must be designed, which allow visitors to connect to the internet and should not be able to exploit Campus network to gain access to internal systems.
10. **Ensuring Network Integrity**
    a. Bidder to ensure that university data is not tampered with or altered as it is critical for maintaining the accuracy and reliability of information stored and transmitted over the network.
    b. Security measures must be incorporated, which help maintain network performance and reliability by protecting against attacks that can degrade service quality or availability.
    c. Bidder must implement robust authentication methods (e.g., 802.1X with RADIUS) to verify user identities and control access to the network integrated with AD/LDAP. Implement access control policies to ensure that users have appropriate permissions, and that guest access is properly managed and isolated.
    d. Segment the network into VLANs to isolate different types of traffic and protect sensitive areas from general network access.
    e. All proposed technology must integrate with deployed campus NGFW to monitor and control incoming and outgoing network traffic, preventing unauthorized access and attacks.
11. **Network testing**
    a. Bidder must perform quarterly check for network robustness and traffic handling and detail report must be submitted every quarter to IT Department of University

4. Eligibility Criteria

4.1 Bidder Eligibility Criteria

1. **Bidder Turnover Criteria**: The minimum average annual financial turnover of the bidder during the last three years, ending on 31st March of the previous financial year should be more than or equal to 100 Crores. Documentary evidence in the form of certified audited balance sheet of relevant period or a certificate from the charted accountant/cost accountant indicating the turnover details for the relevant period shall be uploaded with the bid. In case the date of constitution/ incorporation of the bidder is less than 3 years, the average turnover in respect of the completed financial years after the date of constitution shall be taken into account for this criterion.
2. The bidder must have a registered firm as per companies act 2013 (as on 31/3/2024). Kindly attach the Certificate of Incorporation and profile of the company along with PAN and GST.
3. **Bidder Experience Criteria**:

   A. The bidder should have suppled, installed and commissioned similar category products during preceding 3 financial years (i.e. current year and three previous financial years) as on bid opening date, as per following criteria:

   i. Single order of at least 35% of estimated bid value; or

   ii. Two orders of at least 20% each of estimated bid value; or

   iii. Three orders of at least 15% of estimated bid value.

   B. The bidder should have executed at least 02 similar work of networking/ Wi-Fi during preceding 3 financial years (i.e. current year and three previous financial years) as on bid opening date.

   (Note - Satisfactory Performance certificate issued by respective Buyer Organization for the above orders should be submitted with bid.)
4. Latest and Valid Quality certifications - ISO 9001, ISO 27001, ISO 20000, CMMI 5.
5. The bidder must have at least 100+ technical Team, the HR must certify the same and share the details like – PF etc. to prove the claim.
6. Bidder should have positive net worth per years in last 3 Years.
7. The bidders should not have been blacklisted by Central or State Govt. The Quoted OEM by the bidder should also not have been blacklisted in last Five years.

8. Bidder financial standing: The bidder should not be under liquidation, court receivership or similar proceedings, should not be bankrupt. Bidder to upload undertaking to this effect.
9. Escalation Matrix for Service Support: Bidder must provide Escalation Matrix of Telephone Numbers for service support.

4.2 OEM Eligibility Criteria

1. **OEM Turnover Criteria**: The minimum average annual financial turnover during the last three years, ending on 31st March of the previous financial year of the active components OEM (Switches, AP, WLAN/ FW) of the offered product, should be more than or equal to 100 Corers. Documentary evidence in the form of certified audited balance sheets of relevant periods or a certificate from the charted accountant/ cost accountant indicating the turnover details for the relevant period shall be uploaded with the bid. The OEM of active component must be registered in India for more than 15 Years or above, copy registration must be submitted.
2. **OEM Experience Criteria**: The OEM product for active components must have been installed in at least 10 Central Government/State Government/PSU/BFSI in last 5 Years or higher. An undertaking in this regard from the proposed OEM duly signed and stamped by the authorised signatory from OEM shall be furnished by the bidder.
3. **Imported Products**: In case of imported products, OEM or authorized seller of OEM should have a registered office in India to provide after sales service support in India. The certificate to this effect should be submitted.
4. The OEM of the offered product must have valid ISO 9001, ISO 27001, ISO 27017/27018, ISO 14001 certification
5. **Financial Criteria - Net Worth**: Net Worth of the OEM should be positive as per last audited financial statement.
6. **Escalation Matrix** for Service Support: OEM must provide Escalation Matrix of Telephone Numbers for service support.

5. Bid Evaluation and Selection Criteria:

1. This is a Two parts bid.
2. Part 1 – Envelop comprises of EMD (as per clause 7 (I)) and Technical Bid comprises of clause wise EOI/ RFP compliances, Un Priced BOQ with Make and Model No, Datasheet, PQ supporting documents.
3. Part 2 – Envelop comprises of Price Bid in given format only.

   Note: Price bid of the technically qualified bidders shall be opened. No prices to be mentioned for any item in technical bid, otherwise bid shall be summarily rejected. Price bid shall mention the prices in given format without any condition. Any conditional price bid shall be summarily rejected and L2 bidder may consider for award of contract with prior approvals of competent authority.
4. Both the envelops shall be put in third envelope addressing to tendering authority and clearly mention EOI/ RFP Name & No. and the PSU contact details.
5. L-2 bidder will be invariably called for negotiation in addition to the L-1 bidder if it is so decided by the competent authority, in addition to L-1 bidder.
6. This is a fast-track project, in view of its immediate implementation the competent authority may divide the work between L1 and L2 bidders, if it is so decided by the competent authority, in addition to L-1 bidder on L1 prices.
7. In case of any discrepancy found in words and figures of total quoted prices, the quoted unit rate shall consider for calculation of total amount and GST.

6. Other Important Clauses

1. **This EOI/RFP is for limited participation of Central Govt. /State Govt. Public Sector Undertakings only. No private firm/company (even empanelled with any Central Govt. /State Govt. PSU) shall be allowed to participate. The buyer will not open and consider such bids for evaluation.**
2. Only one bid is allowed from each Central Govt. /State Govt. Public Sector Undertakings, in case any PSU submit two or more bids, all the bids of that PSU will be summarily rejected.
3. **Experience Criteria:** The bidder or its OEM of active components (themselves or through reseller(s)) should have regularly, manufactured and supplied same or similar category products to any Central/State Govt Organizations/ PSU before the bid

opening date. Copies of relevant contracts/ undertaking from active component OEM in this regard to be submitted along with bid in support of having supplied some quantity during each of the last 3 years. Three Years of Past Experience Required for Same/Similar Products.

4. The bidder/OEM should have implemented Wireless Access Points single work order of at least 200 Access Points in single purchase order to fulfil the work experience. The necessary supporting document/ undertaking from OEM needs to furnish by bidder.
5. **Availability of service centres**: Bidder/OEM must have a 24x7 functional service centre in the state of each consignee's location in case of carry-in warranty. (Not applicable in case of goods having on-site warranty).
6. Dedicated/toll free telephone no. for service support: Bidder/OEM must have dedicated/toll free telephone no. for service support.
7. **Proof for Past Experience and Project Experience Clause**: For fulfilling the experience criteria any one of the following documents may be considered as valid proof for meeting the experience criteria:
    - **i.** Contract copy along with Invoice(s) with self-certification by the bidder that service/supplies against the invoices have been executed.
    - **ii.** Execution certificate by client with contract value.
    - iii. Any other document in support of contract execution like Third party inspection lease note, undertaking from OEM etc.
8. Actual delivery, installation & commissioning (if covered in scope of supply) is to be carried out at following address “e-Governance Nodal Centre, Sambalpur University, Jyoti Vihar, Burla, Sambalpur, Odisha.”
9. The Campus has Perimeter & Gateway security being managed by Fortinet Appliance FG-201F and which has built-in Wireless Controller. The Bidder may quote Wireless devices wherein Gateway Security device can be utilized. The bidder must ensure any additional Hardware or Licenses if need must be part of the Complete Solution being provisioned and proposed.
10. All Active components like: Switches, Indoor & Outdoor Access Points and WLAN Controller must be from same OEM. The Bidder must ensure Central management solution is supplied along to centrally manage all components like: Ethernet Switches,

Indoor and Outdoor Access Points and Central Management Solution must also manage existing Perimeter Next Generation SWC

11. Bidder shall quote only those products (part of service delivery) in the bid which are not obsolete in the market and has at least 5 years residual market life. i.e. The offered product shall not be declared end-of-life by the OEM before this period.
12. Malicious Code Certificate: The bidder shall upload following certificate from active components OEM in the bid:
    a. This is to certify that the Hardware and the Software being offered, as part of the contract, does not contain Embedded Malicious code that would activate procedures to: -
        i. Inhibit the desires and designed function of the equipment.
        ii. Cause physical damage to the user or equipment during the exploitation.
        iii. Tap information resident or transient in the equipment/network.
    b. The firm will be considered to be in breach of the procurement contract, in case physical damage, loss of information or infringements related to copyright and intellectual property right (IPRs) are caused due to activation of any such malicious code in embedded software.
13. Bidder are advised to check applicable GST on their own before quoting. Buyer will not take any responsibility in this regard. GST reimbursement will be as per actuals or as per applicable rate (whichever is lower); subject or maximum of quoted GST%.
14. Datasheet of the product(s) offered in the bid, are to be uploaded along with the EOI documents. Buyer can match and verify the Datasheet with the product specifications offered. in case of any unexplained mismatch of technical parameters, the bid is liable for rejection.
15. **End User Certificate**: Wherever bidders are insisting for End User Certificate from the Buyer, same shall be provided in Buyer standard format only.
16. Installation, Commissioning, Testing, Configuration, Training (if any-whichever is applicable as per scope of supply) is to be carried out by OEM/OEM Certified resource or OEM authorised Reseller.
17. All Transceivers/Optics both Copper & Fibre must from same OEM as Active Components

18. IT equipment shall be IPv6 ready from day one.
19. Bidders offer is liable to be rejected if they don't upload any of the certificate/documents sought in the bid document, ATC, corrigendum, addendum if any.
20. **Manufacturer Authorization**: Wherever authorised distributors/service providers are submitting the bid, authorisation form/certificate with OEM/Original Service Provider details such as name, designation, address, e-mail id and phone no. required to be furnished along with the bid.
21. The bidder is advised to visit and examine the installation site and its surrounding and obtain for itself on its own responsibility all information that may be necessary for preparing the bid. The costs of visiting the site shall be borne by the bidder.
22. The bidder representative shall be allowed entry upon consignee premisses for such visits, only upon the express conditions that the bidder will release and indemnify the buyer and consignee against all liabilities arising out of such visit including death or injury, loss or damage to property and any other loss, damage, costs and expenses incurred as a result of such visit.
23. The bidder shall not be entitled to hold any claim against buyer for noncompliance due to lack of any kind of pre-requisite information as it is the sole responsibility of the bidder to obtain all the necessary information with regard to site, surrounding, working conditions, weather etc. on its own before submission of the bid.
24. Products supplied shall be nontoxic and harmless to health. In the case of toxic materials, material safety data sheet may be furnished along with the material.
25. The buyer has an existing setup/inventory similar product. The offered/supplied product must be compatible with existing system. The bidder has to ensure compatibility of the supplied items or shall have to include in the supply the necessary hardware/software to make them compatible.
26. The successful bidder has to supply all essential accessories required for successful installation and commissioning of the goods supplied. Besides standard accessories as per normal industry practice, following accessories must be part of supply and cost should be included in bid price.
27. The bidder shall not sub-contract the contract in whole or part to any entity without obtaining prior written consent of buyer. The decision of the competent authority shall

be final in this regard. At the same time, in case the bidder has any pre bid arrangement/ agreement with any partner/ agency/ company, the bidder has to furnish the detail of partner/ agency/ company in the bid. Such partner/ agency/ company need to comply to minimum 50% of bidder's TO criteria and must be a profitable legal entity with positive net worth. The bidder has to ensure the compliance. At any stage of contract execution, any non-compliance shall lead to termination of contract and bidder shall be barred from participation in future bids for minimum 5 years. In such scenario, the work shall be carried out by the buyer on the risk and cost of the bidder.

28. **Site Survey before bid submission:** this is allowed only for prospective PSUs/ its ONE authorised partner/ agency/ company, who has been on boarded by PSU as part of pre bid arrangement/ agreement. Only ONE partner/ agency/ company per PSU shall be allowed for site survey on behalf of PSU, in case such partner/ agency/ company has been onboarded by PSU before bid participation by Central Govt./ State Govt. No other partner/ agency/ company shall be entertained without PSU authorisation and a supporting document in this regard.
29. Without prejudice to buyer's right to price adjustment by way of discount or any other right or remedy available to buyer. Buyer may terminate the contract or any part thereof by a written notice to the seller, if:
    a. The seller fails to comply with any material term of the contract.
    b. The seller informs buyer of its inability to deliver the material(s) or any part thereof within the stipulated delivery period or such inability otherwise becomes apparent.
    c. The seller fails to deliver the material(s) or any part thereof within stipulated delivery period and/or to replace/rectify any rejected or defective material(s) promptly.
    d. The seller becomes bankrupt or goes into liquidation.
    e. The seller makes a general assignment for the benefit of creditors.
    f. A receiver is appointed for any substantial property owned by the seller.
    g. The seller has misrepresented to Buyer, acting on which misrepresentation buyer has placed the purchase order on the seller.

30. Warranty period of the supplied products shall be 3 years from the date of final acceptance of goods or after completion of installation, commissioning & testing of goods (if included in the scope of supply), at consignee location. OEM warranty certificates must be submitted by Successful Bidder at the time of delivery of goods. The seller should guarantee the rectification of goods in case of any break down during the guarantee period. Seller should have well established installation, commissioning, training, troubleshooting and maintenance service group in India for attending the after sales service. Details of service centre near consignee destinations are to be uploaded with the bid. In case site is not ready the Warranty will start and no payment of the Bidder/OEM will be with-hold.
31. Successful bidder will have to ensure that adequate number of dedicated technical service personals/engineers are designated/deployed for attending to the service request in a time bound manner and for ensuring timely servicing/ rectification of defects during warranty period.
32. Timely servicing/rectification of defects during warranty period: After having been notified of the defects/ service requirement during warranty period, seller has to complete the required service/ rectification within 3 days' time limit. if the seller fails to complete service/rectification with defined time limit, a penalty of 0.5% of unit price of the product shall be charged as penalty for each week of delay from the seller. Seller can deposit the penalty with the buyer directly else the buyer shall have a right to recover all such penalty amount from the performance security (PBG). Cumulative Penalty cannot exceed more than 10% of the total contract value after which buyer shall have the right to get the service/rectification done from alternate sources at the risk and cost of the seller besides forfeiture of PBG. Seller shall be liable to re-imburse the cost of such service/rectification to Buyer.
33. **Quantity Variation:** The Buyer has right to increase or decrease the BOQ quantity of any line item to +/- 25% from the given BOQ quantity without any price variation. Any factional quantity shall be rounded off to next whole no.
34. **Price Validity:** The bidder has to furnish an undertaking regarding the price validity for quoted prices for at least 1 year from the date of singing of the agreement. The buyer is free to place the repeat order within 1 year. Also, in case of any drastic change (>= to 5%) in global currencies (USD/ EURO/ Pond etc.) due to unforeseen factor needs to

account for during the placement of repeat order after 180 days and within 1 year from the date of singing of agreement. The variation on either side shall be justified with due supporting calculation/ documents and benefit needs to pass to effecting party. The amount payable/ receivable shall be only the differential amount on account of currency variation

35. **Resident Engineer:** For smooth operations and maintenance, the bidder has to ensure a RE at site during O&M/ Warranty period for full 3 years from Go-Live date. The bidder may consider the cost of the RE in their bid.
36. **Presentation during bid evaluation:** Presentation shall be an essential part of technical bid evaluation criteria and bidder has to present in front of technical committee. The cost involved in presentation at client site has to be borne by the bidder. Any deviation found by technical committee during presentation in the proposed solution by bidder and bid requirement by buyer shall lead to outrightly rejection of bid without citing any reasons. Hence, bidder must read the EOI/ RFP document and understand document, scope of work and project delivery very thoroughly before quoting.

7. Forms of EMD and PBG

I. Bidders should submit the EMD @ 2% the bid value from any nationalized bank with Account Payee Demand Draft/ Bankers Cheque/ RTGS/ Bank Guarantee in favour of **Comptroller of Finance, Sambalpur University, State Bank of India Jyoti Vihar Burla, Sambalpur**. Bidder has to upload scanned copy/proof of the DD along with bid and has to ensure delivery of hardcopy to the buyer within 3 days of bid end date. Bids of those bidders shall be considered to open whose EMD has been received by SU in stipulated time. EMD of successful bidder shall be returned after submission of PBG as mentioned in clause (II) below. EMD of all the other participated bidder shall be returned after award of contract to successful bidders.

II. Bidders should submit the PBG @5% of the project value from nationalized banks valid for a period of 36 months in favour of Comptroller of Finance, Sambalpur University payable at State Bank of India Jyoti Vihar Burla. The bidder has to ensure delivery of hardcopy to the buyer within 30 days of award of contract.

III. EMD shall be exempted for the PSU registered with MSME/NSIC.

8. Payment Terms:

I. 50% of project value as advance against advance BG of equivalent amount. 28% against material delivery on Pro-rata basis. 10% of project value against Installation and Commissioning and against Go-Live.

II. Balance 12% equally payable quarterly (1% per quarter) in over O&M period of 3 years.

III. **Order/ BoQ Quantities:** The buyer shall place the single order as per given BoQ quantity in EOI/ RFP document but the buyer is free to ask for scattered delivery/ part delivery as per site readiness, phase wise project requirements. The bidder has to adhere to such instructions given to bidder by competent authority. However, the entire BoQ quantity needs to deliver in not more than 6 months from date of signing off of the contract by the bidder.

9. Arbitration and Dispute

In the event of any dispute or difference arising under this agreement or in connection therewith (except as to the matter, the decision to which to which is specifically provided under this agreement) the same shall be referred to the a bench of three arbitrators, of which one arbitrator shall be appointed by each party and third arbitrator shall be appointed by mutual consent of two arbitrators. The agreement to appoint an arbitrator and proceedings of arbitration shall be in accordance with the Arbitration and Conciliation Act 1996.

The arbitrator may from time to time with the consent of both the parties; enlarge the time frame for making and furnishing the award. Subject to the aforesaid, Arbitration and Conciliation Act 1996 and the rules made there under, any modification thereof for the time being in force shall be deemed to apply to the arbitration proceeding under this rule. The seat and venue of the arbitration proceeding shall be Sambalpur or agreed by all the three arbitrators. G

In case of failure of arbitration and any dispute arises out, it shall be admissible to Cuttack High Court, Odisha.

10. Unpriced BoQ with Make & Model

A. Active					
Sr. No.	**Detail Description**	**Qty**	**UOM**	**Make**	**Model**
1	SITC of Layer 3 24 x GE/10GE SFP/SFP+ slots and 2 x 100GE QSFP28. Dual AC power supplies Core Switch (Detail as per mentioned Specification)	2	NOS		
2	SITC of Layer 3 Distribution Switch PoE 802.3bt switch with 24 x 10G/5G/2.5G/1G RJ45 and 2 x 100GE QSFP28 ports. Max 1440W PoE output limit. Dual AC power supplies. (Detail as per mentioned Specification)	8	NOS		
3	SITC of Layer 2 Access with 48 Port and 4x10G SFP+ switch PoE+/FPoE (Detail as per mentioned Specification) – Type-1	25	NOS		
4	SITC of Layer 2 Access with 24 Port and 4x10G SFP+ switch PoE+/FPoE (Detail as per mentioned Specification) – Type-2	71	NOS		
5	SITC of Layer 2 Access switch 48 Port and 4x1G SFP Switch PoE+/FPoE (Detail as per mentioned Specification) – Type-3	25	NOS		
6	SITC of Layer 2 Access switch 24 Port and 4x1G SFP Switch PoE+/FPoE (Detail as per mentioned Specification) – Type-4	85	NOS		
7	SITC of Internet Switch Layer 2/3 24 GE RJ45, 4x 1 G SFP ports (Detail as per mentioned Specification)	2	NOS		
8	SITC of Indoor Wireless AP - Tri radio (Wi-Fi-6E IEEE 802.11ax Tri-band 2.4/5/6GHz and dual 5G operation 4+4+4 4 streams 3 radios), internal antennas, 2x 5G Base-T RJ45, BT/BLE, 1x Type A USB, 1x RS-232 RJ45 Serial Port. Ceiling/wall mount kit included. (Detail as per mentioned Specification)	870	NOS		

9	SITC of Outdoor Access Point - Tri radio (1x 802.11b/g/n/ax 4x4 radio, 1 x 802.11a/n/ac/ax 4x4 Radio and 1x 802.11 a/b/g/n/ac/ax 6GHz, 2x2), 1x 10/100/1000/2500/10000 Base-T RJ45, 1x 10/100/1000 Base-T RJ45, BT/BLE + Zigbee, , 1x RS-232 RJ45 Serial Port. External Dual Band N-Type Omni Directional antennas, Integrated mounting bracket for Antenna included + Wall/Pole Mount mounting kit. Ships with PoE injector. (Detail as per mentioned Specification)	82	NOS		
10	SITC of Secure Wireless Controller with Additional Functionality like Authenticator & restrict unauthorized or non-compliant devices and users from accessing the Campus network. It must enable privilege access and Zero Trust Policies and Strategies. (Detail as per mentioned Specification) (a). Dedicated centralized management with automation-driven network configuration, visibility, and security policy management. (b). Dedicated gatekeeper of authorization identifying users, querying access permissions (c). Dedicated Network Access Controller for Providing advanced protection against IoT threats, protection of sensitive data and vital assets, Users. (Detail as per mentioned Specification)	2	NOS		
11	SITC of 1GE SFP RJ45 transceiver module for systems with SFP and SFP/SFP+ slots	20	NOS		
12	SITC of 1GE SFP SX transceiver module for systems with SFP and SFP/SFP+ slots	20	NOS		
13	SITC of 40 GE QSFP+ passive direct attach cable, 1m for systems with QSFP+/QSFP28 slots.	2	NOS		
14	SITC of 10GE SFP+ transceiver module, 10km long range for systems with SFP+ and SFP/SFP+ slots	88	NOS		
15	SITC of 10GE SFP+ transceiver module, short range 10GE SFP+ transceiver module, short range for systems with SFP+ and SFP/SFP+ slots	245	NOS		
16	SITC of 10GE SFP+ active direct attach cable, 10m / 32.8 ft for systems with SFP+ and SFP/SFP+ slots	3	NOS		

B. Passive BOQ:					
Sr. No.	**Product Description**	**Qty**	**UOM**	**Make**	**Model**
1	SITC of 4U Network Rack	5	NOS		
2	SITC of 12U Rack	133	NOS		
3	SITC of 42U Rack	3	NOS		
4	Supply & Laying of Cat 6 Cable	179950	MTRS		
5	SITC of 24 Port Jack Pannel Loaded	160	NOS		
6	SITC of Cat 6 I/O	2800	NOS		
7	SITC of Cat 6 Patch Cord 1M	2800	NOS		
8	SITC of CAT 6 Patch Cord 2M	2800	NOS		
9	SITC of Dual Port Faceplate	1400	NOS		
10	SITC of Surface Mount Box	1400	NOS		
11	Supply & laying of 24 Core Fiber Cable Single mode	4500	MTRS		
12	Supply & laying of 24 Core Fiber Cable Multimode	5500	MTRS		
13	Supply & laying of 12 Core Fiber Cable Multimode	16500	MTRS		
14	SITC of 24 Port LIU loaded LC Multimode	58	NOS		
15	SITC of 48 Port LIU loaded LC Single mode	12	NOS		
16	SITC of 48 Port Loaded LIU Multimode	40	NOS		
17	SITC of 3 Mtrs Fiber Patch Cord Multimode LC to LC	245	NOS		
18	SITC of 3 Mtrs Fiber Patch Cord Single mode LC to LC	50	NOS		
19	Supply & laying of 1"Casing Patti	5100	MTRS		
20	Supply & laying of 2"Casing Patti	2300	MTRS		
21	SITC of 1"Flexible Bundle	152	NOS		
22	SITC of 2"Flexible Bundle	78	NOS		
23	SITC of Screw Box	365	BOX		
24	SITC of Raul Plug	1095	BOX		
25	SITC of 10 MM Fasteners.	524	NOS		
26	SITC of 1/2" Full Thread Screw	25	BOX		
27	SITC of 1" PVC Pipe with accessories	2450	NOS		
28	SITC of 45*45 PVC Channel BOX	730	NOS		
29	SITC of RJ 45 Connectors	1500	NOS		
30	SITC of Cable Tie 200mm	730	PCKT		
31	Supply & laying of 25MM HDEP Pipe	23500	MTRS		

32	SITC of Outdoor Pole - 3" Width & Height - 15 feet (for Outdoor AP Mounting) with proper RCC foundation.	30	NOS		
33	SITC of Ferrol	5000	NOS		

C. Electrical Work:					
Sr. No.	**Description**	**QTY**	**UOM**	**Make**	**Model**
1	Supply & laying of 2.5sq. Mm, 3 core cable.	4425	MTRS		
2	SITC of 8 Model box with plate, switch and plug	137	NOS		
3	SITC of 1" Casing Patti	1836	NOS		
4	SITC of Screw box	150	NOS		
5	SITC of Raul Plug	150	PCKT		
6	SITC of Electric Tape.	10	BOX		
7	SITC of Rack Chemical Earthing	140	NOS		

D. Digging Work:			
Sr. No.	**Service Description**	**Qty**	**UOM**
1	Digging (HDD/ Molling/ Open) and refurbishment of Soil (Rocky/ Hard/ Soft) with laying of 25mm duct as per CPWD/ PWD Standards/ norms	22000	MTRS

E. Civil Work:			
Sr. No.	**Description**	**Qty**	**UOM**
1	SITC of Main Hole per 150 mts	150	NOS

F.UPS:					
Sr. No.	**Product Description**	**Qty**	**UOM**	**Make**	**Model**
1	SITC of UPS with Inbuilt Battery with 60 mins battery backup	140	NOS		
2	SITC of Supporting Stand for UPS	140	NOS		

G. Support Services			
Sr.no	**Description**	**Qty**	**UOM**
1	O&M and CMC charges after Go live for Three Year	3	YEAR
2	Residential Engineer for 3 Year's	3	YEAR

H. Miscellaneous Items:			
Sr.no	**Description**	**Qty**	**UOM**
1	Miscellaneous Items (if any other than above line items like Ofc route marker at distance of 50 mts each etc.)	1	LOT

Note:

1. The bidder has to mandatorily quote/mention make and model no. against
   a. Active BOQ - Sr. No. 1 to 16;
   b. Passive BOQ - Sr. No. 1, 2, 3, 4, 7, 8, 11, 12, 13, 14, 15, 16, 17, 18 & 31;
   c. Electrical Work - Sr. No. 1 & 2 and
   d. UPS - Sr. No. 1
2. The Bidder has to quote/ mention only single Make & Model No against desired line items mentioned above in Note 1.

11. Technical Specifications

11.1 Technical Specifications for Core Switch

Sl. No.	**Specification Core Switch**	**Compliance (Yes/No)**
1	Should have 24x GE/10GE SFP+ ports and 2x 40GE / 100GE QSFP+ / QSFP28 ports, 1RU	
2	Should have 880Gbps of Switching capacity or more	
3	Should have 1309 Mpps of Packets Forwarding or more	
4	Should have 64K or more MAC address table	
5	Should have 4K or more VLAN support	
6	Should support at least 24 Link Aggregation, 8 Queues, 8GB Memory, 32MB Flash, 8GB SSD or higher from Day 1	
7	Dual hot swappable AC Power Supply,	
8	The Ethernet switch being proposed must be a Secure Access switches deliver a Secure, Simple, Scalable Ethernet solution with outstanding security, performance and manageability for threat.	
9	Switch should support in-built network access control feature to bounce all the devices by default in onboarding VLAN and based on the devices matching with the specified criteria devices should be assigned to a specific VLAN. Criteria: a.MAC address, b. hardware vendor, c. device family, d. device type, e. device operating system and user group. In case, above mentioned functionality is not in-built in the switch bidder can provide additional required hardware and software	

	resources of same OEM whose switches are proposed to meet the mentioned functionality.	
10	Switch should support simple management access i.e. without the need for local management clients (HTTPS preferred)	
11	Switch should have option to allow administrators to quarantine hosts and users connected to a Switch via GUI. Quarantined MAC addresses should be isolated from the rest of the network and LAN. In case, above mentioned functionality is not in-built in the switch above can provide additional required hardware and software resources of same OEM whose switches are proposed to meet the mentioned functionality.	
12	Should have management protocol that allows Gateway/Perimetric Security Appliance to seamlessly manage any Ethernet Switch	
13	Switch should support SNMP for polling of system statistics, SNMP traps, SNMP MIB download from GUI	
14	Should log all authentication events Locally and to Syslog Server	
15	Should support backup of the full system configuration via the GUI	
16	Should support a local user database	
17	Should have built-in tcpdump-like tool and log collecting functionality	
18	Should support REST API for configuration and monitoring	
19	Should support auto-ranging power supply with input voltages between 100 and 240V AC	
20	Should support jumbo frames	
21	Should support link auto-negotiation	
22	Should support Spanning Tree Protocol, STP Root Guard, BPDU Guard	
23	Should support Edge Port / Port Fast	
24	Should support IEEE 802.1p Mapping to priority queue and VLAN tagging	
25	Should support IEEE 802.3ad Link Aggregation with LACP	
26	Should support load balancing algorithms with Link Aggregation	
27	Should support MCLAG (Multi Chassis Link Aggregation)	
28	Should support Auto Discovery of Multiple Switches from central management system	
29	Should support 802.1x MAC-based authentication	
30	Should support MAC Authentication Bypass (MAB)	
31	Should support load balancing algorithms with Link Aggregation	
32	Should support virtual wire	

33	Should support full line rate without traffic oversubscription	
34	Should support Time-Domain Reflectcometry (TDR) Support, this will be used for testing cable systems and able to detect and pinpoint issues	
35	Should support telnet/SSH	
36	Should support SNTP	
37	Should support firmware download via TFTP/FTP/GUI	
38	Should support Policy-Based Routing from central management system	
39	Should support Policy Control of Users and Devices from central management system	
40	Should support Blacklisting and While Listing of MAC address from central management system	
41	Should support Storm Control	
42	Should support Loop Guard	
43	Should support IGMP snooping	
44	Should support DHCP snooping and DHCP relay	
45	Should support Port mirroring	
46	Should support security checks	
47	Should support port MAC limit	
48	Should support MAC-IP binding	
49	Should support static MAC	
50	Should support Dynamic ARP Inspection	
51	Should support Sticky Mac	
52	Should support IEEE 802.1p Based Priority Queuing	
53	Should support packet classification, packet marking, packet queuing	
54	Should support 802.1p, TOS/DSCP for priority queueing	
55	Should support strict scheduling mode, Round Robin (RR), Weighted Round Robin (WRR)	
56	Should support policer	
57	Should support QoS per VLAN	
58	Should support Dynamic Routing Protocols OSPFv2, RIPv2, VRRP, BGP, ISIS	
59	Should support Bidirectional Forwarding Detection (BFD) and VRP	
60	Should support IP Conflict Detection and Notification	
61	Should have Certification & Compliance - FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2	

11.2 Technical Specifications for Distribution Switch

Sl. No.	Specification Distribution Switch	Compliance (Yes/No)
1	Should have Layer 2/3 switch controller compatible PoE 802.3bt switch with 24 x 10G/5G /2.5G /1G RJ45 and 2 x 40/100GE QSFP28 ports. Max 1440W PoE output limit, 1RU	
2	Should have 880Gbps of Switching capacity or more	
3	Should have 1309 Mpps of Packets Forwarding or more	
4	Should have 64K or more MAC address table	
5	Should have 4K or more VLAN support	
6	Should support at least 24 Link Aggregation, 8 Queues, 8GB Memory, 32MB Flash, 8GB SSD	
7	Dual hot swappable AC Power Supply,	
8	The Ethernet switch being proposed must be a Secure Access switches deliver a Secure, Simple, Scalable Ethernet solution with outstanding security, performance and manageability for threat.	
9	Switch should support in-built network access control feature to bounce all the devices by default in onboarding VLAN and based on the devices matching with the specified criteria devices should be assigned to a specific VLAN, Criteria: a.MAC address, b. hardware vendor, c. device family, d. device type, e. device operating system and user group. In case, above mentioned functionality is not in-built in the switch bidder can provide additional required hardware and software resources of same OEM whose switches are proposed to meet the mentioned functionality.	
10	Switch should support simple management access i.e. without the need for local management clients (HTTPS preferred)	
11	Switch should have option to allow administrators to quarantine hosts and users connected to a Switch via GUI. Quarantined MAC addresses should be isolated from the rest of the network and LAN. In case, above mentioned functionality is not in-built in the switch above can provide additional required hardware and software resources of same OEM whose switches are proposed to meet the mentioned functionality.	
12	Should have management protocol that allows Gateway/Perimetric Security Appliance to seamlessly manage any Ethernet Switch	
13	Switch should support SNMP for polling of system statistics, SNMP traps, SNMP MIB download from GUI	

14	Should log all authentication events Locally and to Syslog Server	
15	Should support backup of the full system configuration via the GUI	
16	Should support a local user database	
17	Should have built-in tcpdump-like tool and log collecting functionality	
18	Should support REST API for configuration and monitoring	
19	Should support auto-ranging power supply with input voltages between 100 and 240V AC	
20	Should support jumbo frames	
21	Should support link auto-negotiation	
22	Should support Spanning Tree Protocol, STP Root Guard, BPDU Guard	
23	Should support Edge Port / Port Fast	
24	Should support IEEE 802.1p Mapping to priority queue and VLAN tagging	
25	Should support IEEE 802.3ad Link Aggregation with LACP	
26	Should support load balancing algorithms with Link Aggregation	
27	Should support MCLAG (Multi Chassis Link Aggregation)	
28	Should support Auto Discovery of Multiple Switches from central management system	
29	Should support 802.1x MAC-based authentication	
30	Should support MAC Authentication Bypass (MAB)	
31	Should support load balancing algorithms with Link Aggregation	
32	Should support virtual wire	
33	Should support full line rate without traffic oversubscription	
34	Should support Time-Domain Reflectometry (TDR) Support, this will be used for testing cable systems and able to detect and pinpoint issues	
35	Should support telnet/SSH	
36	Should support SNTP	
37	Should support firmware download via TFTP/FTP/GUI	
38	Should support Policy-Based Routing from central management system	
39	Should support Policy Control of Users and Devices from central management system	
40	Should support Blacklisting and While Listing of MAC address from central management system	
41	Should support Storm Control	
42	Should support Loop Guard	

43	Should support IGMP snooping	
44	Should support DHCP snooping and DHCP relay	
45	Should support Port mirroring	
46	Should support security checks	
47	Should support port MAC limit	
48	Should support MAC-IP binding	
49	Should support static MAC	
50	Should support Dynamic ARP Inspection	
51	Should support Sticky Mac	
52	Should support IEEE 802.1p Based Priority Queuing	
53	Should support packet classification, packet marking, packet queuing	
54	Should support 802.1p, TOS/DSCP for priority queueing	
55	Should support strict scheduling mode, Round Robin (RR), Weighted Round Robin (WRR)	
56	Should support policer	
57	Should support QoS per VLAN	
58	Should support Dynamic Routing Protocols OSPFv2, RIPv2, VRRP, BGP, ISIS	
59	Should support Bidirectional Forwarding Detection (BFD) and VRP	
	Should support IP Conflict Detection and Notification	
	Should have Certification & Compliance - FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2	

11.3 Technical Specifications for Access Switch-Type-1

Sl. No	**Specification Access Switch – Type 1**	**Compliance (Yes/no)**
1	Switch should have 48 x RJ-45 Full POE	
2	Switch should have 4x SFP+ 1/10GbE ports to work with 1/10G SFP transceivers	
3	Switch should provide 176 Gbps of switching capacity	
4	Switch should provide 262 Mpps of throughput	
5	Switch should have a capacity of 32k MAC	
6	Switch should be in the form of 1RU with 19" Rackmount	

7	The Ethernet switch being proposed must be a Secure Access switches deliver a Secure, Simple, Scalable Ethernet solution with outstanding security, performance and manageability for threat.	
8	Switch should support in-built network access control feature to bounce all the devices by default in onboarding VLAN and based on the devices matching with the specified criteria devices should be assigned to a specific VLAN, Criteria: a.MAC address, b. hardware vendor, c. device family, d. device type, e. device operating system and user group. In case, above mentioned functionality is not in-built in the switch bidder can provide additional required hardware and software resources of same OEM whose switches are proposed to meet the mentioned functionality.	
9	Switch should have option to allow administrators to quarantine hosts and users connected to a Switch via GUI. Quarantined MAC addresses should be isolated from the rest of the network and LAN. In case, above mentioned functionality is not in-built in the switch above can provide additional required hardware and software resources of same OEM whose switches are proposed to meet the mentioned functionality.	
10	Switch should provide traffic prioritization (IEEE 802.1p) allows real-time traffic classification into priority levels mapped to queues	
11	Switch should provide layer 4 prioritization based on TCP/UDP port numbers	
12	Switch should provide class of service (CoS) sets the IEEE 802.1p priority tag based on IP address, IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and DiffServ	
13	Switch should provide Rate limiting sets per-port ingress enforced maximums and per-port, per-queue minimums	
14	Should have management protocol that allows Gateway/Perimetric Security Appliance to seamlessly manage any Ethernet Switch	
15	Switch should support IEEE 802.1s Multiple Spanning Tree provides high link availability by allowing multiple spanning trees; provides legacy support for IEEE 802.1d and IEEE 802.1w	
16	Switch should support EEE 802.3ad link-aggregation-control protocol (LACP) and port trunking support up to 26 static, dynamic, or distributed trunks with each trunk having up to eight links (ports) per static trunk	
17	Switch should support SNMPv1, v2, and v3 provide complete; support of industry-standard Management Information Base (MIB) plus private extensions; SNMPv3 supports increased security using encryption	

18	Switch should support dual flash images provide independent primary and secondary operating system files for backup while upgrading	
19	Switch should support custom port names to allow assignment of descriptive names to ports	
20	Switch should have a PoE Power Budget of min 900 W, for connecting Access Points	
21	Switch should have VLAN support and tagging supports IEEE 802.1Q (4,094 VLAN IDs) and 512 VLANs simultaneously	
22	Switch should support jumbo packets to improves the performance of large data transfers; supported frame size of up to 9,220 bytes	
23	Switch should support Rapid per-VLAN spanning tree (RPVST+) to allows each VLAN to build a separate spanning tree to improve link bandwidth usage; is compatible with PVST+	
24	Switch should support DHCP server to centralize and reduces the cost of IPv4 address management	
25	Switch should support static IP routing to provide manually configured routing	
26	Switch should use an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server to authenticate in accordance with industry standards	
27	Switch should support multiple IEEE 802.1X users per port to provide authentication of multiple devices on a single port, which will prevent a user from piggybacking on another user's IEEE 802.1X authentication	
28	Switch should support RADIUS/TACACS+ to ease switch management security administration by using a password authentication server	
29	Switch must have option to ping using Switch serial number instead of the Switch IP address.	
30	Switch should support secure shell encryption for all transmitted data for secure remote CLI access over IP networks	
31	Switch should support Secure Sockets Layer (SSL) encryption for all HTTP traffic, allowing secure access to the browser-based management GUI in the switch	
32	All the solution should be managed by the central manager which can manages 1000 devices which includes AP and Switches and if central management is unavailable, it must have capability to get managed through proposed firewall itself.	

33	Security functionalities allowed to be extended till the access port. Proposed Firewall, Endpoint Security, Core & access Switches, Access points should be preferably from single OEM in case of multiple OEM's solution integration to be built by bidders.	
34	Switches should be capable of providing visibility to the devices connected into the connected ports	
35	Switch must support Operating Temperature 0°C to 50°C from Day 1	
36	Certification & Compliance - FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2	

11.4 Technical Specifications for Access Switch – Type-2

Sl. No.	Specification Access Switch – Type 2	Compliance (Yes/No)
1	Switch should have 24 x RJ-45 Full POE	
2	Switch should have 4x SFP+ 1/10GbE ports to work with 1/10G SFP transceivers.	
3	Switch should provide 128 Gbps of switching capacity	
4	Switch should provide 190 Mpps of throughput	
5	Switch should have a capacity of 16k MAC	
6	Switch should be in the form of 1RU with 19" Rackmount	
7	The Ethernet switch being proposed must be a Secure Access switches deliver a Secure, Simple, Scalable Ethernet solution with outstanding security, performance and manageability for threat.	
8	Switch should provide traffic prioritization (IEEE 802.1p) allows real-time traffic classification into priority levels mapped to queues	
9	Switch should provide layer 4 prioritization based on TCP/UDP port numbers	
10	Switch should provide class of service (CoS) sets the IEEE 802.1p priority tag based on IP address, IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and DiffServ	
11	Switch should provide Rate limiting sets per-port ingress enforced maximums and per-port, per-queue minimums	
12	Should have management protocol that allows Gateway/Perimetric Security Appliance to seamlessly manage any Ethernet Switch	
13	Switch should support IEEE 802.1s Multiple Spanning Tree provides high link availability by allowing multiple spanning trees; provides legacy support for IEEE 802.1d and IEEE 802.1w	

14	Switch should support EEE 802.3ad link-aggregation-control protocol (LACP) and port trunking support up to 26 static, dynamic, or distributed trunks with each trunk having up to eight links (ports) per static trunk	
15	Switch should support SNMPv1, v2, and v3 provide complete; support of industry-standard Management Information Base (MIB) plus private extensions; SNMPv3 supports increased security using encryption	
16	Switch should support dual flash images provide independent primary and secondary operating system files for backup while upgrading	
17	Switch should support custom port names to allow assignment of descriptive names to ports	
18	Switch should have a PoE Power Budget of min 400 W, for connecting Access Points	
19	Switch should have VLAN support and tagging supports IEEE 802.1Q (4,094 VLAN IDs) and 512 VLANs simultaneously	
20	Switch should support jumbo packets to improves the performance of large data transfers; supported frame size of up to 9,220 bytes	
21	Switch should support Rapid per-VLAN spanning tree (RPVST+) to allows each VLAN to build a separate spanning tree to improve link bandwidth usage; is compatible with PVST+	
22	Switch should support DHCP server to centralize and reduces the cost of IPv4 address management	
23	Switch should support static IP routing to provide manually configured routing	
24	Switch should use an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server to authenticate in accordance with industry standards	
25	Switch should support multiple IEEE 802.1X users per port to provide authentication of multiple devices on a single port; which will prevent a user from piggybacking on another user's IEEE 802.1X authentication	
26	Switch should support RADIUS/TACACS+ to ease switch management security administration by using a password authentication server	
27	Switch must have option to ping using Switch serial number instead of the Switch IP address.	

28	Switch should support in-built network access control feature to bounce all the devices by default in onboarding VLAN. And Based on the devices matching with the specified criteria devices should be assigned to a specific VLAN. Criteria: a.MAC address, b. hardware vendor, c. device family, d. device type, e. device operating system and user group. If bidder not supported in-built, they should include all the required hardware and software resources.	
29	Switch should support secure shell encryption for all transmitted data for secure remote CLI access over IP networks	
30	Switch should support Secure Sockets Layer (SSL) encryption for all HTTP traffic, allowing secure access to the browser-based management GUI in the switch	
31	All the solution should be managed by the central manager which can manages 1000 devices which includes AP and Switches and if central management is unavailable, it must have capability to get managed through proposed firewall itself.	
32	Security functionalities allowed to be extended till the access port. Proposed Firewall, Endpoint Security, Core & access Switches, Access points should preferably from single OEM in case of multiple OEM's solution integration to be built by bidders.	
33	Switches should be capable of providing visibility to the devices connected into the connected ports	

11.5 Technical Specifications for Access Switch - Type 3

Sl. No	Specification Access Switch - Type 3	Compliance (Yes/no)
1	Switch should have 48 x RJ-45 Full POE, 740W PoE Power	
2	Switch should have dedicated additional 4x 1GE SFP ports to work with 1G SFP transceivers	
3	Switch should provide 104 Gbps of switching capacity	
4	Switch should provide 155 Mpps of throughput	
5	Switch should have a capacity of 16k MAC	
6	Switch should be in the form of 1RU with 19" Rackmount	
7	The Ethernet switch being proposed must be a Secure Access switches deliver a Secure, Simple, Scalable Ethernet solution with outstanding security, performance and manageability for threat.	

8	Switch should support in-built network access control feature to bounce all the devices by default in onboarding VLAN and based on the devices matching with the specified criteria devices should be assigned to a specific VLAN. Criteria: a.MAC address, b. hardware vendor, c. device family, d. device type, e. device operating system and user group. In case, above mentioned functionality is not in-built in the switch bidder can provide additional required hardware and software resources of same OEM whose switches are proposed to meet the mentioned functionality.	
9	Switch should have option to allow administrators to quarantine hosts and users connected to a Switch via GUI. Quarantined MAC addresses should be isolated from the rest of the network and LAN. In case, above mentioned functionality is not in-built in the switch above can provide additional required hardware and software resources of same OEM whose switches are proposed to meet the mentioned functionality.	
10	Switch should provide traffic prioritization (IEEE 802.1p) allows real-time traffic classification into priority levels mapped to queues	
11	Switch should provide layer 4 prioritization based on TCP/UDP port numbers	
12	Switch should provide class of service (CoS) sets the IEEE 802.1p priority tag based on IP address, IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and DiffServ	
13	Switch should provide Rate limiting sets per-port ingress enforced maximums and per-port, per-queue minimums	
14	Should have management protocol that allows Gateway/Perimetric Security Appliance to seamlessly manage any Ethernet Switch	
15	Switch should support IEEE 802.1s Multiple Spanning Tree provides high link availability by allowing multiple spanning trees; provides legacy support for IEEE 802.1d and IEEE 802.1w	
16	Switch should support EEE 802.3ad link-aggregation-control protocol (LACP) and port trunking support up to 26 static, dynamic, or distributed trunks with each trunk having up to eight links (ports) per static trunk	
17	Switch should support SNMPv1, v2, and v3 provide complete; support of industry-standard Management Information Base (MIB) plus private extensions; SNMPv3 supports increased security using encryption	
18	Switch should support dual flash images provide independent primary and secondary operating system files for backup while upgrading	

19	Switch should support custom port names to allow assignment of descriptive names to ports	
20	Switch should have a PoE Power Budget of min 740 W, for connecting Access Points	
21	Switch should have VLAN support and tagging supports IEEE 802.1Q (4,094 VLAN IDs) and 512 VLANs simultaneously	
22	Switch should support jumbo packets to improves the performance of large data transfers; supported frame size of up to 9,220 bytes	
23	Switch should support Rapid per-VLAN spanning tree (RPVST+) to allows each VLAN to build a separate spanning tree to improve link bandwidth usage; is compatible with PVST+	
24	Switch should support DHCP server to centralize and reduces the cost of IPv4 address management	
25	Switch should support static IP routing to provide manually configured routing	
26	Switch should use an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server to authenticate in accordance with industry standards	
27	Switch should support multiple IEEE 802.1X users per port to provide authentication of multiple devices on a single port, which will prevent a user from piggybacking on another user's IEEE 802.1X authentication	
28	Switch should support RADIUS/TACACS+ to ease switch management security administration by using a password authentication server	
29	Switch must have option to ping using Switch serial number instead of the Switch IP address.	
30	Switch should support secure shell encryption for all transmitted data for secure remote CLI access over IP networks	
31	Switch should support Secure Sockets Layer (SSL) encryption for all HTTP traffic, allowing secure access to the browser-based management GUI in the switch	
32	All the solution should be managed by the central manager which can manages 1000 devices which includes AP and Switches and if central management is unavailable, it must have capability to get managed through proposed firewall itself.	
33	Security functionalities allowed to be extended till the access port. Proposed Firewall, Endpoint Security, Core & access Switches, Access points should be preferably from single OEM in case of multiple OEM's solution integration to be built by bidders.	

34	Switches should be capable of providing visibility to the devices connected into the connected ports	
35	Switch must support Operating Temperature 0°C to 50°C from Day 1	
36	Certification & Compliance - FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2	

11.6 Technical Specifications for Access Switch - Type 4

Sl. No.	Specification Access Switch - Type 4	Compliance (Yes/No)
1	Switch should have 24 x RJ-45 Full POE	
2	Switch should have dedicated additional 4x 1GE SFP ports to work with 1G SFP transceivers	
3	Switch should provide 56 Gbps of switching capacity	
4	Switch should provide 83 Mpps of throughput	
5	Switch should have a capacity of 8k MAC	
6	Switch should be in the form of 1RU with 19" Rackmount	
7	The Ethernet switch being proposed must be a Secure Access switches deliver a Secure, Simple, Scalable Ethernet solution with outstanding security, performance and manageability for threat.	
8	Switch should provide traffic prioritization (IEEE 802.1p) allows real-time traffic classification into priority levels mapped to queues	
9	Switch should provide layer 4 prioritization based on TCP/UDP port numbers	
10	Switch should provide class of service (CoS) sets the IEEE 802.1p priority tag based on IP address, IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and DiffServ	
11	Switch should provide Rate limiting sets per-port ingress enforced maximums and per-port, per-queue minimums	
12	Should have management protocol that allows Gateway/Perimetric Security Appliance to seamlessly manage any Ethernet Switch	
13	Switch should support IEEE 802.1s Multiple Spanning Tree provides high link availability by allowing multiple spanning trees; provides legacy support for IEEE 802.1d and IEEE 802.1w	
14	Switch should support EEE 802.3ad link-aggregation-control protocol (LACP) and port trunking support up to 26 static, dynamic, or distributed trunks with each trunk having up to eight links (ports) per static trunk	
15	Switch should support SNMPv1, v2, and v3 provide complete; support of industry-standard Management Information Base (MIB) plus private extensions; SNMPv3 supports increased security using encryption	
16	Switch should support dual flash images provide independent primary and secondary operating system files for backup while upgrading	
17	Switch should support custom port names to allow assignment of descriptive names to ports	
18	Switch should have a PoE Power Budget of min 400 W, for connecting Access Points	

19	Switch should have VLAN support and tagging supports IEEE 802.1Q (4,094 VLAN IDs) and 512 VLANs simultaneously	
20	Switch should support jumbo packets to improves the performance of large data transfers; supported frame size of up to 9,220 bytes	
21	Switch should support Rapid per-VLAN spanning tree (RPVST+) to allows each VLAN to build a separate spanning tree to improve link bandwidth usage; is compatible with PVST+	
22	Switch should support DHCP server to centralize and reduces the cost of IPv4 address management	
23	Switch should support static IP routing to provide manually configured routing	
24	Switch should use an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server to authenticate in accordance with industry standards	
25	Switch should support multiple IEEE 802.1X users per port to provide authentication of multiple devices on a single port; which will prevent a user from piggybacking on another user's IEEE 802.1X authentication	
26	Switch should support RADIUS/TACACS+ to ease switch management security administration by using a password authentication server	
27	Switch must have option to ping using Switch serial number instead of the Switch IP address.	
28	Switch should support in-built network access control feature to bounce all the devices by default in onboarding VLAN. And Based on the devices matching with the specified criteria devices should be assigned to a specific VLAN. Criteria: a.MAC address, b. hardware vendor, c. device family, d. device type, e. device operating system and user group. If bidder not supported in-built, they should include all the required hardware and software resources.	
29	Switch should support secure shell encryption for all transmitted data for secure remote CLI access over IP networks	
30	Switch should support Secure Sockets Layer (SSL) encryption for all HTTP traffic, allowing secure access to the browser-based management GUI in the switch	
31	All the solution should be managed by the central manager which can manages 1000 devices which includes AP and Switches and if central management is unavailable, it must have capability to get managed through proposed firewall itself.	
32	Security functionalities allowed to be extended till the access port. Proposed Firewall, Endpoint Security, Core & access Switches, Access points should preferably from single OEM in case of multiple OEM's solution integration to be built by bidders.	
33	Switches should be capable of providing visibility to the devices connected in to the connected ports	

11.7 Technical Specifications for L3 Internet Switch

Sl. No.	Specification Internet Switch	Compliance (Yes/No)
1	Should have Layer 2/3 switch controller compatible switch with 24 GE RJ45, 4x 10 GE SFP + ports, 1RU	
2	Should have 128Gbps of Switching capacity or more	
3	Should have 190 Mpps of Packets Forwarding or more	
4	Should have 16K or more MAC address table	
5	Should have 4K or more VLAN support	
6	Should support at least 24 Link Aggregation, 8 Queues, 1GB DDR4 Memory, 256MB Flash, MTB >10 Years, Network Latency < 1µs	
7	Dual hot swappable AC Power Supply,	
8	The Ethernet switch being proposed must be a Secure Access switches deliver a Secure, Simple, Scalable Ethernet solution with outstanding security, performance and manageability for threat.	
9	Switch should support simple management access i.e. without the need for local management clients (HTTPS preferred)	
10	Should have management protocol that allows Gateway/Perimetric Security Appliance to seamlessly manage any Ethernet Switch	
11	Switch should support SNMP for polling of system statistics, SNMP traps, SNMP MIB download from GUI	
12	Should log all authentication events Locally and to Syslog Server	
13	Should support backup of the full system configuration via the GUI	
14	Should support a local user database	
15	Should have built-in tcpdump-like tool and log collecting functionality	
16	Should support REST API for configuration and monitoring	
17	Should support auto-ranging power supply with input voltages between 100 and 240V AC	
18	Should support jumbo frames	
19	Should support link auto-negotiation	
20	Should support Spanning Tree Protocol, STP Root Guard, BPDU Guard	
21	Should support Edge Port / Port Fast	
22	Should support IEEE 802.1p Mapping to priority queue and VLAN tagging	
23	Should support IEEE 802.3ad Link Aggregation with LACP	
24	Should support load balancing algorithms with Link Aggregation	

25	Should support MCLAG (Multi Chassis Link Aggregation)	
26	Should support Auto Discovery of Multiple Switches from central management system	
27	Should support 802.1x MAC-based authentication	
28	Should support MAC Authentication Bypass (MAB)	
29	Should support load balancing algorithms with Link Aggregation	
30	Should support virtual wire	
31	Should support full line rate without traffic oversubscription	
32	Should support Time-Domain Reflectcometry (TDR) Support, this will be used for testing cable systems and able to detect and pinpoint issues	
33	Should support telnet/SSH	
34	Should support SNTP	
35	Should support firmware download via TFTP/FTP/GUI	
36	Should support Policy-Based Routing from central management system	
37	Should support Policy Control of Users and Devices from central management system	
38	Should support Blacklisting and While Listing of MAC address from central management system	
39	Should support Storm Control	
40	Should support Loop Guard	
41	Should support IGMP snooping	
42	Should support DHCP snooping and DHCP relay	
43	Should support Port mirroring	
44	Should support security checks	
45	Should support port MAC limit	
46	Should support MAC-IP binding	
47	Should support static MAC	
48	Should support Dynamic ARP Inspection	
49	Should support Sticky Mac	
50	Should support IEEE 802.1p Based Priority Queuing	
51	Should support packet classification, packet marking, packet queuing	
52	Should support 802.1p, TOS/DSCP for priority queueing	
53	Should support strict scheduling mode, Round Robin (RR), Weighted Round Robin (WRR)	
54	Should support policer	

55	Should support QoS per VLAN	
56	Should support Dynamic Routing Protocols OSPFv2, RIPv2, VRRP, BGP, ISIS	
57	Should support Bidirectional Forwarding Detection (BFD) and VRP	
58	Should support IP Conflict Detection and Notification	
59	Should have Certification & Compliance - FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2	

11.8 Technical Specifications for Indoor Access Point

Sl. No.	**Specification for Indoor Access point (with Omni Directional External Antennas from Day 1)**	**Compliance (Yes/No)**
1	The Access Point should support 802.11ax wifi-6 standard, built-in onboard Security functions like Application control and Web filtering	
2	Must have the Tri-radio option to support radio1 as 2.4 GHz and radio2 as 5 GHz devices and radio 3 as 2.4GHz/5 GHz for frequency scanning.	
3	Should have x4 Dual band Wi-Fi, x4 Tri-band Wi-Fi and Scanning, 1x2.4GHz BLE/ ZigBee, 1 GPS antenna	
4	Should have minimum x2 100/1000/2500/5000 Base-T RJ45, 1 Type 3.0 USB, 1 RS-232 RJ45 Serial Port	
5	AP should support 25 W without PSE out and 37.9 W with PSE out POE power.	
6	Should support Wave 4x4 MU-MIMO	
7	The access Point should support throughput in Radio 1: up to 1147 Mbps, Radio 2: up to 2402 Mbps, Radio 3: Up to 4804 Mbps	
8	Should support Peak antenna gain of minimum 5.5 dBi in 2.4 GHz and 7.2 dBi in 5 GHz band, BLE antenna: 5.0 dBi in 2.4 GHz band With PCB patch GPS active antenna: 2.2dBi antenna	
9	Access point should support SSID's in Tunnel, Bridge, Split-Tunnel and mesh mode.	
10	Should support 16 Simultaneous SSIDs	
11	Should support following EAP types: EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST	
12	Access point should support IEEE standards 802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i,802.11j, 802.11k, 802.11n, 802.11r, 802.11v, 802.11w, 802.11ac, 802.11ax (Wi-Fi 6), 802.1Q, 802.1X, 802.3ad, 802.3af, 802.3at, 802.3az, 802.3bt, 802.3bz	

13	Should Support per Radio Capacity Up to 512 clients per radio (Radio1, Radio2 and Radio3)	
14	Must Support User or Device Authentication like - WPA™, WPA2™, and WPA3™ with 802.1x or Preshared key, WEP, Web Captive Portal, MAC blocklist and allowlist	
15	Should have physical security lock (such as Kensington lock)	
16	Should support mounting options of Wall and Pole mounting kit with all the accessories must include with box.	
17	Access point should support below Wireless Monitoring Capabilities	
18	a) Rogue Scan Radio Modes should support both background and dedicated	
19	b) WIPS / WIDS Radio Modes should support both background and dedicated	
20	c) should support Spectrum Analyzer	
21	d) should support Packet Sniffer Mode	
22	Must support Reliable Multicast Video to maintain video quality	
23	Must support QoS and Call Admission Control capabilities.	
24	Access point should have static option to mention 3 controller ip address to discover the controller for redundancy.	
25	The access point must support wireless mesh to eliminate the need for Ethernet wiring by connecting Wi-Fi access points to the controller by radio.	
26	Aps must have two Ethernet port that operates as a WAN port to provide management connection to a Wi-Fi Controller and another LAN to provide a wired network access.	
27	Should support Local AP diagnostic web portal, Command line (CLI) directly to access point.	
28	Access point Operating Temperature should be: -40–140°F (-40°C - 50°C)	
29	Access point must include power supply 802.3bt PoE, injector.	
30	Access point should support IP67 rating and Mean Time Between Failures > 10 Years.	
31	Access point should support Surge Protection Built In.	
32	All Access points, Switches, Firewall, Secure Controller, Authenticator/RADIUS Server, NAC etc. must be preferably from same OEM	

11.9 Technical Specifications for Outdoor Access Point

Sl. No	Specification for Outdoor Access point (with Omni Directional External Antennas from Day 1)	Compliance (Yes/No)
1	The Access Point should support 802.11ax wifi-6 standard, built-in onboard Security functions like Application control and Web filtering	
2	Must have the Tri-radio option to support radio1 as 2.4 GHz and radio2 as 5 GHz devices and radio 3 as 2.4GHz/5 GHz for frequency scanning.	
3	Should have 4 dual band Wi-Fi + 1 dual band scanning + 1 single band 2.4 GHz BLE/ZigBee	
4	Should have minimum 1x 100/1000/2500 Base-T RJ45, 1 x 10/100/1000 Base-T RJ45 (802.3af PoE PSE), 1x RS-232 RJ45 Serial Port	
5	AP should support 25 W without PSE out and 37.9 W with PSE out POE power.	
6	Should support Wave 4x4 MU-MIMO	
7	The access Point should support throughput in Radio 1: up to 1147 Mbps, Radio 2: up to 2402 Mbps, Radio 3: Up to 4804 Mbps	
8	Should support Peak antenna gain of minimum 5.5 dBi in	
9	2.4 GHz and 7.2 dBi in 5 GHz band, BLE antenna: 5.0 dBi in 2.4 GHz band	
10	With PCB patch GPS active antenna: 2.2dBi antenna	
11	Access point should support SSID's in Tunnel, Bridge, Split-Tunnel and mesh mode.	
12	Should support 16 Simultaneous SSIDs	
13	Should support following EAP types: EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST	
14	Access point should support IEEE standards 802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i,802.11j, 802.11k, 802.11n, 802.11r, 802.11v, 802.11w, 802.11ac, 802.11ax (Wi-Fi 6), 802.1Q, 802.1X, 802.3ad, 802.3af, 802.3at, 802.3az, 802.3bt, 802.3bz	
15	Should have physical security lock (such as Kensington lock)	
16	Should support mounting options of Wall and Pole mounting kit with all the accessories must include with box. If not quote all mounting kit.	
17	Access point should support below Wireless Monitoring Capabilities	
18	a) Rogue Scan Radio Modes should support both background and dedicated	
19	b) WIPS / WIDS Radio Modes should support both background and dedicated	
20	c) should support Spectrum Analyzer	

21	d) should support Packet Sniffer Mode	
22	Must support Reliable Multicast Video to maintain video quality	
23	Must support QoS and Call Admission Control capabilities.	
24	Must Support User or Device Authentication like - WPA™, WPA2™, and WPA3™ with 802.1x or pre-shared key, WEP, Web Captive Portal, MAC blocklist and allowlist	
25	Access point should have static option to mention 3 controller ip address to discover the controller for redundancy.	
26	The access point must support wireless mesh to eliminate the need for Ethernet wiring by connecting Wi-Fi access points to the controller by radio.	
27	Aps must have two Ethernet port that operates as a WAN port to provide management connection to a Wi-Fi Controller and another LAN to provide a wired network access.	
28	Should support Local AP diagnostic web portal, Command line (CLI) directly to access point.	
29	Access point Operating Temperature should be: -40–140°F (-40°C - 60°C)	
30	Access point must include power supply 802.3bt PoE, injector.	
31	Access point should support IP67 rating and Mean Time Between Failures > 10 Years.	
32	Access point should support Surge Protection Built In.	
33	All Access points, Switches, Firewall, Secure Controller, Authenticator/RADIUS Server, NAC etc. must be preferably from same OEM	

11.10 Technical Specifications for WLAN Controller

Sl. No.	Specifications of Secure WLAN Controller	Compliance (Yes / No)
1	The SWC should be Hardware based, Reliable, purpose-built security WLAN Controller appliance with hardened operating system that eliminates the security risks associated with general-purpose operating systems and should have dual internal power supply from day one. SWC Controller must support 1000 or higher Access Points from day 1	
2	The Proposed Vendor must be present in Leader's Quadrant of Gartner Magic Quadrant for Enterprise Wired & Wireless.	

3	SWC appliance should have at least 16 x 1GE interfaces, 4 x 1GbE SFP slot and 2x 10G SFP+ slot	
4	SWC device Should have Throughput of at least 150 Gbps	
5	SWC appliance should support minimum 50 Gbps or higher for VPN throughput	
6	SWC appliance should support 2000 site-to-site & at least 50000 or higher client to site VPN Tunnels.	
7	SWC appliance should support minimum 10000 concurrent SSL VPN users and should be scalable in future	
8	SWC device must support 700,000 or higher new sessions per second	
9	SWC device must support at least 15 million concurrent sessions or higher	
10	SWC should have minimum Latency equal or less than 4µs	
11	The SWC device solution must support minimum 20 Gbps of SWC (FW + IPS + AVC) throughput for Mix / production traffic	
12	The SWC device solution must minimum 20 Gbps of Threat Prevention (FW + IPS + AVC + AV) throughput for Mix / production traffic or higher from day 1	
13	Should have built in Virtual WAN architecture & functionality to leverage any combination of transport services — including MPLS, LTE and broadband internet services	
14	The SWC solution should support NAT64, NAT46, DNS64 & DHCPv6	
15	The proposed system should have integrated Traffic Shaping functionality.	
16	The SWC & IPSEC VPN module shall belong to product family which minimally attain Internet Computer Security Association (ICSA) Certification.	
17	The proposed system should support signatures should a severity level defined to it so that it helps the administrator to understand and decide which signatures to enable for what traffic (e.g. for severity level: high medium low)	
18	b) PPTP VPN	
19	c) L2TP VPN	
20	The device shall utilize inbuilt hardware VPN acceleration:	
21	a) IPSEC (DES, 3DES, AES) encryption/decryption	
22	b) SSL encryption/decryption	
23	The system shall support the following IPSEC VPN capabilities:	

24	a) Multi-zone VPN supports.	
25	b) IPSec, ESP security.	
26	c) Supports NAT traversal	
27	d) Supports Hub and Spoke architecture	
28	e) Supports Redundant gateway architecture	
29	The system shall support 2 forms of site-to-site VPN configurations:	
30	a) Route based IPSec tunnel	
31	b) Policy based IPSec tunnel	
32	The system shall support IPSEC site-to-site VPN and remote user VPN in transparent mode.	
33	The system shall provide IPv6 IPSec feature to support for secure IPv6 traffic in an IPSec VPN.	
34	**Virtualization**	
35	The proposed solution should support Virtualization (Virtual SWC, Security zones and VLAN). Minimum 10 Virtual license (VDOM) should be provided from Day1.	
36	**Intrusion Prevention System**	
37	IPS throughput should be minimum 25 Gbps for Mix / Production traffic or higher from Day 1	
38	The IPS detection methodologies shall consist of:	
39	a) Signature based detection using real time updated database	
40	b) Anomaly based detection that is based on thresholds	
41	The IPS system shall have at least 15,000 signatures	
42	IPS Signatures can be updated in three different ways: manually, via pull technology or push technology. Administrator can schedule to check for new updates or if the device has a public IP address, updates can be pushed to the device each time an update is available	
43	In event if IPS should cease to function, it will fail open by default and is configurable. This means that crucial network traffic will not be blocked and the SWC will continue to operate while the problem is resolved	
44	IPS solution should have capability to protect against Denial of Service (DOS) and DDOS attacks. Should have flexibility to configure threshold values for each of the Anomaly. DOS and DDOS protection should be applied, and attacks stopped before SWC policy lookups.	

45	IPS signatures should have a configurable action like terminate a TCP session by issuing TCP Reset packets to each end of the connection, or silently drop traffic in addition to sending an alert and logging the incident	
46	Signatures should a severity level defined to it so that it helps the administrator to understand and decide which signatures to enable for what traffic (e.g. for severity level: high medium low)	
47	**Antivirus**	
48	SWC should have integrated Antivirus solution if not please quote separate appliance	
49	The proposed system should be able to block, allow or monitor only using AV signatures and file blocking based on per SWC policy based or based on SWC authenticated user groups with configurable selection of the following services:	
50	a) HTTP, HTTPS	
51	b) SMTP, SMTPS	
52	c) POP3, POP3S	
53	d) IMAP, IMAPS	
54	e) FTP, FTPS	
55	The proposed system should be able to block or allow oversize file based on configurable thresholds for each protocol types and per SWC policy.	
56	**Web Content Filtering**	
57	The proposed system should have integrated Web Content Filtering solution without external solution, devices or hardware modules.	
58	The proposed solution should be able to enable or disable Web Filtering per SWC policy or based on SWC authenticated user groups for both HTTP and HTTPS traffic.	
59	The proposed system shall provide web content filtering features:	
60	a) which blocks web plug-ins such as ActiveX, Java Applet, and Cookies.	
61	b) Shall include Web URL block	
62	c) Shall include score-based web keyword block	
63	d) Shall include Web Exempt List	
64	The proposed system shall be able to queries a real time database of over 110 million + rated websites categorized into 70+ unique content categories.	
65	**Application Control**	

66	The proposed system shall have the ability to detect, log and take action against network traffic based on over 3000 application signatures	
67	The application signatures shall be manual or automatically updated	
68	The administrator shall be able to define application control list based on selectable application group and/or list and its corresponding actions	
69	The vendor should have their own threat intelligence centre for all security services and don't depend on a third party for security update	
70	Standards-based secure authentication which works to deliver secure two-factor authentication to any third-party device capable of authentication via RADIUS or LDAP	
71	SWC must have integrable hardware appliance which can be deployed in minutes to secure access to your existing network infrastructure	
72	The System should support minimum 1500 Local Users + Remote Users and scalable to 3500 from Day 1	
73	Should support at least 10 User Groups or more	
74	The appliance should have a manageability over CLI and Console and HTTPS.	
75	The system should support SNMP v1 / v2c / v3.	
76	Should support at least 5 SYSLOG Servers.	
77	The system should support at least 10 numbers of Static-Routes	
78	Integrates with existing solutions such as LDAP or AD servers to lower the cost and complexity of adding strong authentication to your network	
79	Support for E-mail and SMS tokens enables rapid deployment of two-factor authentication without the need for additional dedicated hardware	
80	Support for Certificate Authority functionality to simplify the CA management and to deliver user certificate signing, VPN, or server x.509 certificates for use in certificate-based two-factor authentication	
81	Single Sign-On (SSO) Transparent User Identification with zero impact for enterprise users	
82	SSO Portal based authentication with tracking widgets to reduce the need for repeated authentications	
83	Solution should be proposed with privileged access for at least 5 users which introduce zero trust principles to privileged accounts and	

	dramatically lower an organizations overall attack surface by integrating user credential with MFA	
84	Solution must support end-to-end management of privileged accounts, control of privileged user access, and visibility of account usage including monitoring and audit capabilities.	
85	Solution must have built in DLP support to prevent any leak of confidential information. Also, must support Antivirus scanning. If DLP and antivirus is not part of PAM solution, then 3rd party solution must be provided which can integrate with PAM solution	
86	Solution should provide full controls of all resource secrets through administrator-defined central policies. These must include options for automatic password changes after check-in. Solution must implement a hierarchical approval system and control risky commands.	
87	Solution should have single agent which work with quoted Firewall SSL VPN agent so that multiple agents is not required at endpoint	
88	Should support SAML SP/IdP Web SSO	
89	Monitoring of Carrier RADIUS Accounting Start records	
90	Proposed solution should form a part of centralized intelligence grid as of network firewall, web application firewall and switches Solution seamlessly share threat intelligence across different vectors as dedicated security platform and must provide this intelligence to centralized management and analysis engine.	
91	Security grid must have automation capability to create key stitches using integrations out of the box for firewalls, web application firewall and switches which should be monitored basis regular triggers to provide automated action capability.	
92	Proposed solution should have native integration with proposed NGFW, Web application firewall and endpoint security solution as authenticator source and must enforce second factor of authentication to ensure zero trust network access.	
93	**High Availability**	
94	The proposed system shall have built-in high availability (HA) features without extra cost/license or hardware component	
95	The device shall support stateful session maintenance in the event of a fail-over to a standby unit.	
96	High Availability Configurations should support Active/Active or Active/ Passive	

97	**Logs and Report**	
98	Should have 480 GB of SSD Drive Capacity for logging and reporting if not please quote separate appliance	
99	Real-time display of information allows you to follow real-time trends in network usage such as the source IP address and the destination URL for HTTP traffic.	
100	All accessories required for deployment of the product in HA should be provided by the bidder.	
101	SWC must support: NAT64, NAT46, DHCPv6 and DNS64 from day one for seamless transition between IPv4 and IPv6.	
102	SWC must support bi-directional communication with dedicated on-premises/cloud based sandboxing solution to share unknown/zero-day content and receive threat intelligence from Sandbox for automated mitigation of attacks. But it should be from same OEM.	
103	SWC solution should support custom IPS signatures and should also have at-least CVE IPS 15,000 signatures or higher from Day 1.	
104	SWC solution should provide protection with security engines like protocol decoders, anomaly detection and should have rate based, pattern based, behavioural based and support for custom defined signatures. It should also ensure defence against exploits and vulnerabilities.	
105	Individual SWC appliances and the Centralized Management and Logging solution should have GUI based management solution from the same OEM.	
106	The solution proposed should support in-built Multiple Security Groups provided by the same OEM.	
107	The solution proposed should be latest and should not have been declared end-of-life from the date of commissioning. An undertaking from OEM needs to be provided for the same.	
108	Operating system of SWC solution must support: USGv6 / IPv6, FIPS-140-2, Common criteria EAL4.	
109	SWC solution should support IPv4 - VPN and IPv6 - VPN feature.	
110	The Centralized reporting and logging solution should be able to provide IoC intelligence, Threat Out Break alerts and should be able to provide automated response against triggered incidents. The Central manager with SWC appliance must be able to manage all active devices like – SWC (WLAN Controller), Indoor Access Points, Outdoor Access	

	Points, Ethernet Switches and existing Perimeter Gateway Security device.	
111	All Components of central Security platform should work together as a team to share policy, threat intelligence, and application flow information.	
112	The bidder will be responsible for installing and configuring the appliances in HA at the respective locations or if SWC can be integrated with existing Gateway. The bidder should further ensure seamless transition of security and access policies from existing solutions to the new setup, through appropriate technical solution and implementation strategy.	

11.11 Technical Specifications for Cat6 Cable

Sl. No.	Cat6 Cable Specifications	Compliance (Yes/No)
1	It should have a standard of ANSI/TIA-568.2-D	
2	It should be certified PoE: IEEE 802.3bt-2018	
3	It should be CMP and CMR Listed	
4	It should be Bare Copper Wire 23AWG	
5	Cable diameter - in. (mm):	
6	The cable diameter at least should be0.23 (5.8) Nom.	
7	The Nominal cable weight at least should be - lb./kft. (kg/km): 26(38)	
8	The maximum installation tension should be 25(10)	
9	The Minimum bend radius should be - in. (mm): ≥ 4 O.D @-20° C / -4°F	
10	The Insulation should be Polyethylene	
11	The Conductor should be: Bare Copper Wire 23AWG	
12	The Cable diameter at least should be - in. (mm): 0.23 (5.8) Nom. Nominal weight 1000ft reel - lb. (kg): 29.6 (13.44)	

11.12 Technical Specifications for Optical Fiber Cable (OFC)

Sl. No.	Specifications OFC	Compliance (Yes/No)
1	It should be ISO.IEC 11801 - 2nd Edition, AS/ACIF S008, AS/NZS 3080 TIA/EIA 568.3-D, IEC-60793-1, 60793-2 EIA/TIA-492, Telcordia (BELLCORE) GR 20 STDS, EIA 455	
2	The Tube should be Polybutylene Terephthalate (PBT)	
3	Tube Colour Should White	
4	Tube Diameter at least should be 3.0/2.0 mm nominal OD/ID	
5	It should have No of Fibers cores 4/6/8/12/24	

6	The Fiber Colour Sequence should be: Blue, Orange, Green, Brown, Slate (Gray), White, Red, Black, Yellow, Violet, Pink, Aqua	
7	The water Blocking should be: Thixotropic Gel (Tube) Petroleum Jelly (Interstices)	
8	The Core Wrapping should it be Polyester tape / Water swellable tape	
9	The Armouring should be Corrugated Steel Tape Armor (ECCS Tape) Thickness > 0.125mm Peripheral Strength Member: Two steel wires (0.9 mm Dia)	
10	The Ripcord should be Polyester based yarns below armoured tape for easy ripping	
11	The Outer Sheath should be UV Stabilized Polyethylene (HDPE)	
12	The Sheath Thickness at least should be 2.0 mm nominal	
13	The Sheath Colour should be Black	

11.13 Technical Specifications for Patch Cord

Sl. No.	**Patch Cord Specifications for 1 & 2 Mtrs**	**Compliance (Yes/No)**
1	The Commercial Standards should be: ISO/IEC 11801 2nd Ed TIA-568-C.2 Cat 6	
2	The Environmental Standards should be RoHS compliant	
3	It should pass Fire Propagation Tests: UL 444	
4	Conductor Size should be 24 AWG stranded copper wire Nom. O.D.: 0.236 inch	
5	Bend Radius should be 8 x O.D	
6	The Operating Temperature should be -20°C to 60°C	
7	The Minimum operating life should be 200 insertion cycles	
8	The RJ45 Plug Material should be Clear polycarbonate UL94V-0 Boot Material	
9	The RJ45 Plug Dimensions should be compliant with: ISO/IEC 60603-7 and FCC 47 Part 68	
10	The MAX VOLTAGE: 150 VAC (MAX)	
11	The max current should be1.5A @ 25°C	

11.14 Technical Specifications for OFC Patch Cord

SI. NO.	Specifications OFC Patch Cord	Compliance (Yes/No)
1	It should be ISO/IEC 11801-1:2017	
2	It should be ANSI/TIA/ EIA 568.3-D	
3	It should be ANSI/TIA/EIA-492	
4	It should be TELECORDIA GR-409 ICEA - 596	
5	It should have AS/CA S008:2020	
6	It should be Cordage O.D.: 2.0mm+/-0.1mm x 4.1mm +/- 0.2mm	
7	It should be Buffer Diameter: 900µm	
8	It should be Primary Coating: 245µm	
9	It should be Strength Member: Aramid Yarn	
10	It should be Jacket Material: LS0H IEC 61034-1 & 2, IEC-60332-1, IEC-60754-1 & 2	
11	It should be Minimum Bend Radius Install: 3.0cm.	
12	It should be Long Term Bend Radius: 2.0cm	
13	It should be Operating Temperature: -40°C to +85°C	
14	The Colour Matrix should be: OS2 9/125: Yellow, OM1 62.5/125: Orange, OM2 50/125: Gray, OM3 50/125: Aqua, OM4 50/125: EV/Aqua & OM5 50/125: Lime Green	

11.15 Technical Specifications for UPS

SI. No.	Specification UPS	Compliance (Yes/No)
1	The UPS capacity at least should be 2000 VA	
2	The normal voltage should be 220V/230V/240V AC (1Ph+N+PE, 3 Wire)	
3	The Operating Voltage Range should be 100V~300V AC Load Dependent	
4	Operating Frequency Range should be 50 / 60 Hz ± 10% (Auto Sensing)	
5	Power Factor should not more than >0.99	
6	Output Voltage/Power Factor should be 220V / 230V / 240V AC / ±1% / 0.8 Std., 0.9 Optional	
7	The output Frequency should be Auto Sensing 50 / 60 Hz ± 1~10% Sync Mode (Configurable), 50/60 Hz ± 0.1 Hz Battery Mode	
8	DC Voltage at least should have 96V	
9	The Charge Current should be 1A	

10	It should have LCD Indication Input Voltage/Frequency, Output Voltage/Frequency, Battery Voltage, Load Watt/VA and %, Inverter Temperature, Operation Mode such as “Online”, “ON Batt” or on “Bypass”, Fault Codes, Battery & Load Bar graph	
11	The Alarms / Protection Batt. Low, DC High, Inverter Under/Over Voltage, UPS Overload, Short Circuit, Fan Failure and UPS Fault.	
12	The Overload Capability should be ≤ 125% for 10 min, >125-150% for 1 min, >150% for 200 ms	
13	Transfer Time should be C to Battery: 0ms, Inverter to Bypass: 4ms (Typical)	
14	It should certify ISO 9001, ISO 14001, ISO 27001, ISO 45001, ISO 50001, BIS, RoHS	
15	It should have safety compliance of IEC/EN62040-1	
16	The communication should be through RS-232, SNMP / Modbus / Dry Contact / USB / RS-485	

11.16 Technical Specifications for HDPE

Sl. NO.	**Specifications HDPE**	**Compliance (Yes/No)**
1	Density at 27^{o}C (base material) - 940 to 958 Kg/m3	
2	Tensile strength at yield. Speed of testing 50 mm/ minute Min. 20 N/mm2	
3	Wall thickness - Min. 2.00 to Max. 2.30	
4	Outside diameter - 25 mm	
5	Lubricated layer thickness Should be min. 5% of wall thickness	
6	Visual Appearance - Smooth inside & outside surface, free of blisters, shrink, hole, flaking, scratches & roughness. Duct shall be smooth, clean and round. The end shall be clearly cut and shall be square with axis of duct.	
7	Grade - PE100 PN12.5 SDR13.6	

11.17 Technical Specifications for Racks (4U, 12U Wall Mount Rack)

Sl. NO.	**4U, 12U Wall Mount Racks**	**Compliance (Yes/No)**
1	4U 550*400, 12U 600*500 wall mount with front Glass door-CKD/ welded	
2	Door with 4mm toughened glass	
3	five folded 19" rail with 'U' Marking	
4	Material: - Pre-galvanised sheet	
5	top panel with 2 fan mounting provision	
6	cable entry provision in top & bottom panel.	
7	Door: - Easily to change door opening direction (Left, Right side opening)	

8	4U - Useable depth 390mm 12U - Useable depth 490mm	
9	Finish: - Powder coated (RAL 7035)	

11.18 Technical Specifications for Racks -42U

SI. NO.	42U Floor Mount Racks	Compliance (Yes/No)
1	The Manufacturer's factory must be ISO 9001 & 14001 Certified. Copy of ISO 9001 & 14001 must be submitted with bid.	
2	Manufacturer must be a global organization and yearly turnover must be above INR 2,000 Crore (relevant documentary proof has to be submitted along with bid).	
3	Size – 42U 800mmW x 1000mmD with Front and Rear fully perforated door with 3-point cam lock.	
4	Degrees of Ingress Protection, IP 20 according to IEC 60529	
5	Degree of Impact Protection, IK 08 according to IEC 62262	
6	Corrosion Resistance through Salt Spray test according to ISO 9227 for 168 hours' protection	
7	Weight carrying capacity (Certified - 1250 Kg)	
8	Process validations thru' NABL labs	
9	Clean earth system with an Electrolytic Copper 99.99 % Pure, with Leakage current results certifications	
10	Racks to be preferably made out high quality CRCA sheets	
11	1.5 mm CRCA Multi Fold Fabricated Frame	
12	Top Panel to be made of 1.2 mm CRCA and concealed from exterior view. Allows provision for 4 nos. Fan mounting	
13	19" inch rails in each rack - 4 nos. U marked Rails made of 2 mm CRCA sheet.	
14	Doors Front & Rear door Full height flush till top Cover. Absence of Horizontal gap between the door and the top panel. 45-degree oblong pattern on the front door.	

11.19 Technical Specifications LIU

SI. NO.	Specifications LIU	Compliance (Yes/No)
1	It should have 24-48 Port Specification Grade Fiber Enclosure - 1U - Metric fixing kit	
2	It should be 24-48 Port Specification Grade Fiber Enclosure - 1U - US Imperial fixing kit	
3	It should be Universal Splice Tray Carrier kit	
4	It should be Fiber Enclosure (shipped assembled)	
5	It should have Fiber Drawer with port labelling sheet	
6	It should be Adjustable/multi-position copper ground stud/Fiber cable support member clamp	

7	It should be 4 Velcro Straps (3/4” x 8”)	
8	It should be 1 Fiber Management Hub	
9	It should be 4 Patch Cord management loops	
10	It should be Fiber Warning Label	
11	It should be 19” Mounting hardware	
12	It should have Instruction Sheet	
13	It at least should be 16 Gauge Cold Rolled steel.	
14	The finish should be 16 Gauge Aluminium	
15	The weight should be 470mm Enclosure Weight: 5.49kg Shipping Weight: 7.19kg	
16	It should be Black Powder Paint Cable Spools	
17	It should be Thermoplastic UL94V-O Dimensions (HxWxD): 41mm x 432mm x 470mm.	

12. Price Bid Format

A. Active					
Sr. No.	**Detail Description**	**Qty**	**UOM**	**Unit Price**	**Total Amount**
1	SITC of Layer 3 24 x GE/10GE SFP/SFP+ slots and 2 x 100GE QSFP28. Dual AC power supplies Core Switch (Detail as per mentioned Specification)	2	NOS		0
2	SITC of Layer 3 Distribution Switch PoE 802.3bt switch with 24 x 10G/5G/2.5G/1G RJ45 and 2 x 100GE QSFP28 ports. Max 1440W PoE output limit. Dual AC power supplies. (Detail as per mentioned Specification)	8	NOS		0
3	SITC of Layer 2 Access with 48 Port and 4x10G SFP+ switch PoE+/FPoE (Detail as per mentioned Specification)- Type-1	25	NOS		0
4	SITC of Layer 2 Access with 24 Port and 4x10G SFP+ switch PoE+/FPoE (Detail as per mentioned Specification) – Type-2	71	NOS		0
5	SITC of Layer 2 Access switch 48 Port and 4x1G SFP Switch PoE+/FPoE (Detail as per mentioned Specification)-Type-3	25	NOS		0
6	SITC of Layer 2 Access switch 24 Port and 4x1G SFP Switch PoE+/FPoE (Detail as per mentioned Specification)-Type-4	85	NOS		0

7	SITC of Internet Switch Layer 2/3 24 GE RJ45, 4x 1 G SFP ports (Detail as per mentioned Specification)	2	NOS		0
8	SITC of Indoor Wireless AP - Tri radio (Wi-Fi-6E IEEE 802.11ax Tri-band 2.4/5/6GHz and dual 5G operation 4+4+4 4 streams 3 radios), internal antennas, 2x 5G Base-T RJ45, BT/BLE, 1x Type A USB, 1x RS-232 RJ45 Serial Port. Ceiling/wall mount kit included. (Detail as per mentioned Specification)	870	NOS		0
9	SITC of Outdoor Access Point - Tri radio (1x 802.11b/g/n/ax 4x4 radio, 1 x 802.11a/n/ac/ax 4x4 Radio and 1x 802.11 a/b/g/n/ac/ax 6GHz, 2x2), 1x 10/100/1000/2500/10000 Base-T RJ45, 1x 10/100/1000 Base-T RJ45, BT/BLE + Zigbee, , 1x RS-232 RJ45 Serial Port. External Dual Band N-Type Omni Directional antennas, Integrated mounting bracket for Antenna included + Wall/Pole Mount mounting kit. Ships with PoE injector. (Detail as per mentioned Specification)	82	NOS		0
10	SITC of Secure Wireless Controller with Additional Functionality like Authenticator & restrict unauthorized or non-compliant devices and users from accessing the Campus network. It must enable privilege access and Zero Trust Policies and Strategies. (Detail as per mentioned Specification) (a). Dedicated centralized management with automation-driven network configuration, visibility, and security policy management. (b). Dedicated gatekeeper of authorization identifying users, querying access permissions (c). Dedicated Network Access Controller for Providing advanced protection against IoT threats, protection of sensitive data and vital assets, Users. Detail as per mentioned Specification)	2	NOS		0

11	SITC of 1GE SFP RJ45 transceiver module for systems with SFP and SFP/SFP+ slots	20	NOS		0
12	SITC of 1GE SFP SX transceiver module for systems with SFP and SFP/SFP+ slots	20	NOS		0
13	SITC of 40 GE QSFP+ passive direct attach cable, 1m for systems with QSFP+/QSFP28 slots.	2	NOS		0
14	SITC of 10GE SFP+ transceiver module, 10km long range for systems with SFP+ and SFP/SFP+ slots	88	NOS		0
15	SITC of 10GE SFP+ transceiver module, short range 10GE SFP+ transceiver module, short range for systems with SFP+ and SFP/SFP+ slots	245	NOS		0
16	SITC of 10GE SFP+ active direct attach cable, 10m / 32.8 ft for systems with SFP+ and SFP/SFP+ slots	3	NOS		0
Total Amount					0

B. Passive					
Sr. No.	**Detail Description**	**Qty**	**UOM**	**Unit Price**	**Total Amount**
1	SITC of 4U Network Rack	5	NOS		0
2	SITC of 12U Rack	133	NOS		0
3	SITC of 42U Rack	3	NOS		0
4	Supply & Laying of Cat 6 Cable	179950	MTRS		0
5	SITC of 24 Port Jack Pannel Loaded	160	NOS		0
6	SITC of Cat 6 I/O	2800	NOS		0
7	SITC of Cat 6 Patch Cord 1M	2800	NOS		0
8	SITC of CAT 6 Patch Cord 2M	2800	NOS		0
9	SITC of Dual Port Faceplate	1400	NOS		0
10	SITC of Surface Mount Box	1400	NOS		0
11	Supply & laying of 24 Core Fiber Cable Single mode	4500	MTRS		0
12	Supply & laying of 24 Core Fiber Cable Multimode	5500	MTRS		0

13	Supply & laying of 12 Core Fiber Cable Multimode	16500	MTRS		0
14	SITC of 24 Port LIU Loaded LC Multimode	58	NOS		0
15	SITC of 48 Port LIU lorded LC Single mode	12	NOS		0
16	SITC of 48 Port Loaded LIU Multimode	40	NOS		0
17	SITC of 3 Mtrs Fiber Patch Cord Multimode LC to LC	245	NOS		0
18	SITC of 3 Mtrs Fiber Patch Cord Single mode LC to LC	50	Nos		0
19	Supply & laying of 1"Casing Patti	5100	MTRS		0
20	Supply & laying of 2"Casing Patti	2300	MTRS		0
21	SITC of 1"Flexible Bundle	152	NOS		0
22	SITC of 2"Flexible Bundle	78	NOS		0
23	SITC of Screw Box	365	BOX		0
24	SITC of Raul Plug	1095	BOX		0
25	SITC of 10 MM Fasteners.	524	NOS		0
26	SITC of 1/2" Full Thread Screw	25	BOX		0
27	SITC of 1" PVC Pipe with accessories	2450	NOS		0
28	SITC of 45*45 PVC Channel BOX	730	NOS		0
29	SITC of RJ 45 Connectors	1500	NOS		0
30	SITC of Cable Tie 200mm	730	PCKT		0
31	Supply & laying of 25MM HDEP Pipe	23500	MTRS		0
32	SITC of Outdoor Pole - 3” Width & Height - 15 feet (for Outdoor AP Mounting) with proper RCC foundation.	30	NOS		0
33	SITC of Ferrol	5000	NOS		0
Total Amount					0

C. Electrical Work:					
Sr. No.	**Detail Description**	**QTY**	**UOM**	**Unit Price**	**Total Amount**
1	Supply & laying of 2.5 3 core cable.	4425	MTRS		0
2	SITC of 8 Model box with plate, switch and plug	137	NOS		0

3	SITC of 1” Casing Patti	1836	NOS		0
4	SITC of Screw box	150	NOS		0
5	SITC of Raul Plug	150	PCKT		0
6	SITC of Electric Tape.	10	BOX		0
7	SITC of Rack Chemical Earthing	140	NOS		0
Total Amount					0

D. Digging Work:					
Sr. No.	**Service Description**	**QTY**	**UOM**	**Unit Price**	**Total Amount**
1	Digging (HDD/ Molling/ Open) and refurbishment of Soil (Rocky/ Hard/ Soft) with laying of 25mm duct as per CPWD/ PWD Standards/ norms	22000	MTRS		0
Total Amount					0

E. Civil Work:					
Sr. No.	**Detail Description**	**QTY**	**UOM**	**Unit Price**	**Total Amount**
1	SITC of Main Hole per 150 mts	150	NOS		0
Total Amount					0

F.UPS:					
Sr. No.	**Product Description**	**QTY**	**UOM**	**Unit Price**	**Total Amount**
1	SITC of UPS with Inbuilt Battery with 60 mins battery backup	140	NOS		0
2	SITC of Supporting Stand for UPS	140	NOS		0
Total Amount					0

G. Support Services					
Sr.no	**Description**	**QTY**	**UOM**	**Unit Price**	**Total Amount**
1	O&M and CMC charges after go live for Three Year	3	YEARS		0
2	Residential Engineer for 3 Year's	3	YEARS		0
Total Amount					0

H. Miscellaneous Items:					
Sr.no	**Detail Description**	**QTY**	**UOM**	**Unit Price**	**Total Amount**
1	Miscellaneous Items (if any other than above line items like Ofc route marker at distance of 50 mts each etc.)	1	LoT		0
Total Amount					0

SUMMARY		
A	Active BOQ	-
B	Passive BOQ	-
C	Electrical BOQ	-
D	Digging BOQ	-
E	Civil Work	-
F	UPS BOQ	-
G	Support Serv.	-
H	Misc. Items	-
	Total Amount	-
	Tax Amount @ 18%	-
	Grand Total	**-**

Amount in Fig: