

# **Bid Document**

**Bid for Supply, Installation, Testing, Commissioning,  
Integration, Operation & Maintenance of Enterprise  
Wired and Wi-Fi Infrastructure Solution for MMCEC  
(Tender No. HWT25092026)**

**Pre-bid Meeting: 01.10.2026 at 1500 hours**

**Venue for pre-bid meeting :** Gujarat Informatics Ltd, Block No. 2, 2nd Floor, C  
& D Wing, Karmayogi Bhavan, Sector - 10 A, Gandhinagar.

**Last Date of Submission of Bid: 09.10.2026 till 1500 hours**

**Last Date of Submission of Bid Processing Fees & EMD: 09.10.2026 till 1500  
hours**

**Date of Opening of Bid: 09.10.2026 on 1600 hours**

**Bid Processing Fee: Rs. 17,700**

**GUJARAT INFORMATICS LIMITED**

Block No. 2, 2nd Floor,

C & D Wing, Karmayogi Bhavan

Sector - 10 A, Gandhinagar – 382010.

Phone No: 23256022

# 1. Introduction

Gujarat Informatics Limited (GIL), on behalf of the **Gandhinagar Railway and Urban Development Corporation Ltd**, Government of Gujarat (hereinafter referred to as the "Tenderer"), invites online bids from eligible bidders for the **Supply, Installation, Testing, Commissioning, Integration, Operation & Maintenance of Enterprise Wired and Wi-Fi Infrastructure Solution** at designated location, in accordance with the terms, conditions, technical specifications, and requirements contained in this Request for Proposal (RFP).

**Location:**

**Mahatma Mandir Convention and Exhibition Centre**

**Sector 13C, Sector 13, Gandhinagar, Gujarat 382016**

The bidder shall quote for all hardware, software, licenses, subscriptions, implementation services, operation & maintenance services, manpower, accessories, consumables, and all other items necessary for complete execution of the project as specified in this RFP.

The quantities indicated in the BOQ are tentative and intended solely for bid evaluation purposes. The Tenderer does not guarantee procurement of the entire indicated quantities and reserves the right to increase, decrease, omit, or add quantities during execution based on actual requirements.

The proposed solution shall include all hardware, software, licenses, subscriptions, accessories, transceivers, mounting hardware, structured cabling components, power accessories, server/storage infrastructure for log retention, and any other components required for successful implementation and operation of the solution. No additional payment shall be admissible on this account.

## 2. Earnest Money Deposit (EMD)

The bidder shall submit an Earnest Money Deposit (EMD) of ₹ ₹ **70,00,000.00/- (Rupees Seventy Lac only)** in accordance with the provisions of this RFP.

The EMD may be submitted in the form of:

- Demand Draft; or
- Unconditional Bank Guarantee.

The EMD Bank Guarantee shall remain valid for a minimum period of **180 days** from the last date of bid submission.

The EMD shall be submitted in favour of:

**Gujarat Informatics Limited, Block No. 2, 2nd Floor, C & D Wing, Karmayogi Bhavan Sector - 10 A, Gandhinagar - 382010 Gujarat.**

Payable at Gandhinagar.

The EMD shall be issued by:

Any Nationalized Bank, Public Sector Bank, Private Sector Bank, Commercial Bank, Co-operative Bank, or Rural Bank operating in India and having a branch at Ahmedabad or Gandhinagar, in accordance with Finance Department G.R. No. FD/MSM/e-file/4/2024/2859/DMO dated 01/05/2025 and subsequent amendments issued from time to time.

The sealed envelope containing the EMD shall be superscripted as:

**"EMD for Tender No. HWT25092026 for Supply, Installation, Testing, Commissioning, Integration, Operation & Maintenance of Enterprise Wired and Wi-Fi Infrastructure Solution."**

Failure to submit the Bid Processing Fee and EMD within the prescribed timeline shall render the bid non-responsive and liable for rejection.

### **3. RTGS / NEFT Details**

For online payment of Bid Processing Fee and EMD, the following bank details may be used:

The bidder shall upload proof of payment along with the bid.

Gujarat Informatics Limited, Block No. 2, 2nd Floor, C & D Wing, Karmayogi Bhavan Sector - 10 A, Gandhinagar - 382010 Gujarat.

Saving Account No: 50200010918090

IFSC Code: HDFC0000190

Bank Name: HDFC

Bank Branch Address: Sector-16, Gandhinagar

### **4. Performance Bank Guarantee (PBG)**

The Successful Bidder shall furnish a Performance Bank Guarantee (PBG) equivalent to **5% of the total Order/Contract Value** towards due and faithful performance of contractual obligations.

The PBG shall be submitted within **07 working days** from the date of issuance of Letter of Intent (LOI) / Work Order.

The PBG shall:

- Be denominated in Indian Rupees.
- Be in the form of an unconditional Bank Guarantee.
- Be issued by an eligible bank as prescribed by the Finance Department.
- Remain valid up to **90 days beyond completion of the Contract Period**.

The PBG may be invoked by the Tenderer in the event of:

- Breach of contractual obligations.
- Failure to meet SLA requirements.
- Non-performance of services.
- Violation of any material condition of the contract.

The PBG shall be released within thirty (30) days after expiry of its validity, subject to satisfactory completion of all contractual obligations and settlement of all dues.

## 5. Return of EMD

The EMD of unsuccessful bidders shall be returned as promptly as possible as but not later than fifteen (15) days after:

- Expiry of bid validity; or
- Award of contract to the successful bidder and submission of the required PBG, whichever is earlier.

## 6. Extension of Bid Validity

In exceptional circumstances, GIL may request bidders to extend the validity of their bids.

Such request and response shall be made in writing.

A bidder agreeing to the extension shall not be permitted to modify its bid.

## 7. Acceptance of LOI / Work Order

The Successful Bidder shall submit written acceptance of the Letter of Intent (LOI) / Work Order along with the Performance Bank Guarantee within the prescribed timelines.

## 8. Tenderer's Rights

The Tenderer reserves the right to:

- Increase, decrease, omit or add any BOQ item or quantity.
- Accept or reject any bid.
- Cancel or withdraw the tender process at any stage.
- Procure any quantity under the contract as per actual requirement.

No compensation shall be payable to any bidder on account of such actions.

## 9. Interpretation

In the event of any discrepancy between the BOQ, Technical Specifications, Scope of Work, Drawings, Annexures, or any other provisions of the RFP, the interpretation and decision of the Tenderer shall be final and binding upon all bidders.

## 10. Key Information:

|   |                |                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Contact Person | <p>Shri. Maulik Chauhan, GM (Tech &amp; Network)<br/>gm-tech@gujarat.gov.in<br/>Phone no. : 079-232 59238</p> <p>Shri. Prakash Dholakia, GM (Networking)<br/>dgmTech-gil@gujarat.gov.in<br/>Phone no. : 079-232 52026</p> <p>Shri. Jitendra Chauhan, Manager (Networking)<br/>srmgr1-gswan@gujarat.gov.in<br/>Phone no. : 079-232 58155</p> <p>Shri. Jignesh Solanki System Administrator<br/>sysadmin5-gil@gujarat.gov.in</p> |
|---|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**Pre-bid Meeting:**

The pre-bid queries/clarifications, if any, should be submitted in writing to Gujarat Informatics Limited by end of the day of the pre-bid meeting date. Thereafter, the clarifications received from the bidders will not be entertained.

**Pre-Bid meeting date: 01/09/26**

Please address all pre-bid queries and correspondence to

Shri. Maulik Chauhan, GM (Tech & Network)

gm-tech@gujarat.gov.in

Phone no. : 079-232 59238

Shri. Prakash Dholakia, GM (Networking)

dgmTech-gil@gujarat.gov.in

Phone no. : 079-232 52026

Shri. Jitendra Chauhan, Manager (Networking)

srmgr1-gswan@gujarat.gov.in

Phone no. : 079-232 58155

Shri. Jignesh Solanki System Administrator

sysadmin5-gil@gujarat.gov.in

---

## ***SECTION 2***

### ***Eligibility Criteria***

---

## Eligibility Criteria:

| Sr. No | Parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Attachments                                                                                                                                                                                                                                                    |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1      | Bidder should be IT/ITeS Company registered under Indian Companies Act 1956/2013,                                                                                                                                                                                                                                                                                                                                                                              | Certificates of incorporation & Self-Declaration Certificates                                                                                                                                                                                                  |
| 2      | The bidder should have successfully supplied and implemented WIFI Infrastructure Solution in State Government Organizations / Central Government / PSU / Listed Companies / BFSI during the last five (5) years, as per any one of the following criteria:<br>a) One (1) project covering 360 or more Access Points, or<br>b) Two (2) projects, each covering 225 or more Access Points, or<br>c) Three (3) projects, each covering 180 or more Access points. | Details of such projects undertaken along with work order/purchase order copy/clients' completion certification/letter signed/ e-mail issued by authorized signatory or company secretary with the details w.r.t to the clause should be enclosed.             |
| 3      | The bidder must have average annual turnover of Rs. 70 Crore (Minimum) in the last three financial years as on 31st March 2026.                                                                                                                                                                                                                                                                                                                                | The copies of Audited Annual Accounts/Balance Sheet along with Profit & Loss Account and CA Certified Statement with UDIN for last three financial years as on 31st March 2026 shall be attached along with the bid.                                           |
| 4      | The OEM & bidder must have positive Net worth or should be Profit making in any three financial years out of last four Financial Year as on 31st March 2026.                                                                                                                                                                                                                                                                                                   | The copies of CA Certified Statement for last three financial years as on 31st March 2026 shall be attached along with the bid.                                                                                                                                |
| 5      | The quoted products of each OEM should have an average annual related turnover of not less than Rs 174 Crores in in any three financial years out of last four Financial Year as on 31st March 2026. (Wi-Fi Infrastructures, Switch, Firewall)                                                                                                                                                                                                                 | The copies of Audited Annual Accounts/Balance Sheet along with Profit & Loss Account and CA Certified Statement with UDIN for last three financial years as on 31st March 2026 shall be attached along with the bid.                                           |
| 6      | The OEM of proposed product must have supplied Wi-Fi Infrastructure appliance with minimum quantity of 750 Access points during the last five (5) years before the bid opening date.                                                                                                                                                                                                                                                                           | Details of such projects undertaken along with work order/purchase order copy/clients' on-going or completion certification/letter signed/ e-mail issued by authorized signatory or company secretary with the details w.r.t to the clause should be enclosed. |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                     |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7  | The bidder must have one office in Gujarat.                                                                                                                                                                                                                                                                                                                                                                                               | <p>Please upload the copies of any two of the following: Property Tax Bill of last year / Electricity Bills of last one year / Telephone Bills of last one year / G.S.T. Registration / Valid Lease Agreement.</p> <p>In case, bidder does not have office in Gujarat, bidder should give undertaking to open office in Gujarat within 45 days from the date of purchase order.</p> |
| 8  | Bidder and OEM should not be blacklisted/debarred by any state government / central government / PSU in last two years as on last date of bid submission.                                                                                                                                                                                                                                                                                 | Bidder and OEM will have to submit undertaking letter at the time of bidding                                                                                                                                                                                                                                                                                                        |
| 9  | The Bidder and OEM should have a Customer Support Centre which operates 24x7x365 and is capable of troubleshooting 24x7x365 days                                                                                                                                                                                                                                                                                                          | A Self Certified letter with Address                                                                                                                                                                                                                                                                                                                                                |
| 10 | The quoted product must be MTCTE certified.                                                                                                                                                                                                                                                                                                                                                                                               | Valid MTCTE certification shall be submitted for offered products falling under an applicable mandatory MTCTE notification.                                                                                                                                                                                                                                                         |
| 11 | The OEM shall comply with the Government of India guidelines regarding restrictions on procurement from bidders/OEMs of countries sharing land borders with India, as applicable and amended from time to time. Necessary declarations and supporting documents, if required, shall be submitted in accordance with the applicable Government of India orders                                                                             | Required document with authorized signatory                                                                                                                                                                                                                                                                                                                                         |
| 12 | Bidder will have to submit Self-Declaration letter for acceptance of ATC Given in bid                                                                                                                                                                                                                                                                                                                                                     | Required document with authorized signatory.                                                                                                                                                                                                                                                                                                                                        |
| 13 | Bidder and OEM's Undertaking as per as per format in guidelines published by Ministry of Finance Dept. of Expenditure Public Procurement division dated 23.07.2020                                                                                                                                                                                                                                                                        | Required document with authorized signatory.                                                                                                                                                                                                                                                                                                                                        |
| 14 | The bidder shall submit a Technical Compliance Statement confirming that the proposed solution fully complies with all technical specifications and requirements of this RFP, supported by relevant OEM datasheets, brochures, or official technical documentation. Non-submission of the compliance statement or failure to comply with the prescribed technical specifications and RFP requirements may result in rejection of the bid. | Required document with authorized signatory.                                                                                                                                                                                                                                                                                                                                        |

|    |                                                                                                                       |                                              |
|----|-----------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
| 15 | Escalation Matrix For Support: Bidder & OEM must provide Escalation Matrix                                            | Required document with authorized signatory. |
| 16 | Manufacturer Authorization: The bidder should be authorized by the OEM to quote the bid. (Bid no. must be mentioned). | Required document with authorized signatory. |

---

*SECTION 3*

*SCOPE OF WORK*

---

### 3.1 Objective

The selected bidder shall be responsible for the **Design, Supply, Delivery, Installation, Configuration, Commissioning, Testing, Documentation, Training, and Warranty Support** of a complete **Enterprise Grade Wi-Fi 7 Network Infrastructure** on a turnkey basis at the designated locations.

The work shall include supply and implementation of all active and passive networking components, optical fiber backbone, structured cabling system, wireless infrastructure, network security, network management solution, network racks, accessories, civil works and all incidental items required for successful commissioning of the project, irrespective of whether explicitly mentioned in the Bill of Quantities (BOQ).

The complete network shall be designed, supplied, installed and commissioned as a highly available and resilient campus network architecture with **no single point of failure**. High Availability (HA) shall be achieved through **two physically separate hardware appliances/devices** deployed in a redundant configuration at all critical layers, including Core Switching, Security Appliances, Wireless LAN Controllers (where applicable) and Network Management components. The two redundant devices shall operate in an OEM-supported High Availability mode (Active-Active, Active-Standby or equivalent, as applicable) and shall not be implemented as virtual instances on the same physical hardware or chassis.

Failure of any single hardware device, power supply, uplink or network component shall not result in disruption of network services.

The proposed solution shall be based on an enterprise-grade campus architecture capable of supporting **Wi-Fi 7 (IEEE 802.11be)**, high-speed enterprise applications, centralized management and monitoring, and shall be support a minimum of total **25,000 registered wireless users** and support 8,000 Concurrent users at Convocation centre from day 1.

### 3.2 Site Survey and Network Design

The bidder shall carry out a comprehensive site survey of all locations prior to implementation.

The activities shall include:

- a. Physical verification of all locations.
- b. Assessment of existing network infrastructure.
- c. RF Site Survey for Wi-Fi deployment.
- d. Preparation of Low Level Design (LLD).
- e. Network Architecture Design.
- f. Fiber Route Plan.
- g. Rack Layout Drawings.
- h. Cable Routing Plan.

- i. AP Placement Layout.
- j. Predictive and Active Wi-Fi Heat Maps.
- k. Switch Port Allocation Plan.
- l. IP Addressing Plan.
- m. VLAN Design.
- n. Power Requirement Assessment.
- o. Preparation of detailed implementation methodology.

No implementation shall commence without approval of the design documents by the Tenderer.

### **3.3 Supply of Passive Network Infrastructure**

The bidder shall design, engineer, supply, deliver, install, test and commission a complete passive network infrastructure required for establishing the proposed network.

The scope shall include, but not be limited to, optical fiber backbone infrastructure, structured copper cabling system, fiber termination system, information outlets, patching infrastructure, cable management system, network connectivity accessories, conduits, ducts, cable protection system, mounting accessories and all other passive components required for successful implementation of the project.

The structured cabling solution shall support high-speed enterprise networking applications, including **Wi-Fi 7** infrastructure. All passive components shall be sourced from a **single OEM** from the list mentioned in BOM/BOQ and shall be fully compatible with each other, forming a complete end-to-end structured cabling solution.

The bidder shall provide all accessories, consumables, connectors, fastening materials and incidental items necessary for complete installation, testing and commissioning, irrespective of whether individually specified in the BOQ.

### **3.4 Supply of Active Network Components**

The bidder shall supply, install, configure, integrate, test and commission all active network components required for establishing a secure, resilient and centrally managed enterprise network.

The scope shall include all networking, wireless, security, management and connectivity equipment, associated software, operating systems, licenses, subscriptions (where applicable), transceivers, interface modules, mounting accessories, power cords, interconnecting cables and all ancillary components necessary for successful implementation of the project.

The bidder shall ensure seamless integration of all active components into a unified network infrastructure with centralized management, monitoring, security and policy enforcement capabilities.

All equipment shall be supplied with the latest stable firmware/software releases, valid licenses, and OEM-supported warranty as specified in the RFP.

### **3.5 Network Rack Infrastructure**

The bidder shall supply, install and commission all types of network racks, enclosures and associated infrastructure required for housing the active and passive network components.

The scope shall include all accessories necessary for proper installation, cable management, power distribution, ventilation, grounding, equipment mounting, physical security, identification and orderly cable routing.

The bidder shall ensure that all racks and enclosures are adequately sized to accommodate the proposed equipment with sufficient spare capacity for future expansion and comply with the applicable industry standards and OEM recommendations.

### **3.6 Installation and Commissioning**

The bidder shall execute complete installation including:

- a. Optical Fiber Cable Laying
- b. HDPE Duct Installation
- c. Copper Cable Laying
- d. PVC Conduit Installation
- e. Flexible Pipe Installation
- f. Rack Installation
- g. LIU Installation
- h. Fiber Splicing
- i. Fiber Termination
- j. Patch Panel Termination
- k. Faceplate Installation
- l. Wireless Access Point Installation
- m. Pole Installation
- n. AP Mounting Clamps
- o. Cable Dressing
- p. Cable Tagging
- q. Labelling of all network elements

### **3.7 Civil and Allied Works**

The bidder shall carry out all civil works necessary for successful implementation including:

- a. Soft Soil Excavation
- b. Trenching

- c. Backfilling
- d. Road Cutting
- e. Concrete Cutting
- f. Wall Cutting
- g. Core Drilling
- h. Surface Restoration
- i. HDPE Duct Installation
- j. PVC Conduit Installation
- k. Pole Foundation
- l. Mounting Structures
- m. Waterproof Sealing
- n. Fire Stopping
- o. Cable Route Protection

The bidder shall restore all disturbed surfaces to their original condition after completion of work.

### **3.8 Configuration and Integration**

The bidder shall configure and integrate all supplied components including:

- a. Firewall Configuration
- b. Security Policies
- c. VLAN Configuration
- d. Layer-2 and Layer-3 Switching
- e. Dynamic Routing
- f. Link Aggregation
- g. High Availability
- h. QoS
- i. Traffic shaping
- j. Network Segmentation
- k. PoE Configuration
- l. Wireless Controller Configuration
- m. Wi-Fi SSIDs
- n. WPA3 Enterprise Security
- o. IEEE 802.1X Authentication
- p. Fast Roaming
- q. Radio Resource Management
- r. RF Optimization
- s. Centralized Monitoring
- t. Alarm Configuration
- u. User Access Policies
- v. Guest user management
- w. Captive Portal management and customization

The entire network shall operate as an integrated solution.

## 3.9 Testing and Acceptance

The bidder shall carry out comprehensive testing including:

### Optical Fiber

The bidder shall carry out **100% testing of all installed optical fiber links** using an **OTDR** and **Optical Loss Test Set (OLTS)/Optical Power Meter and Light Source**, and submit complete test reports. The measured attenuation shall comply with the applicable ITU-T and IEC standards and the OEM's recommended limits.

### Copper Cabling

The successful bidder shall carry out **100% certification testing of all installed copper structured cabling links** using a **Fluke Networks DSX Series Cable Analyzer (DSX-5000/DSX-8000 or higher) or equivalent Level VI/Level 2G compliant field tester**.

The installed cabling shall successfully pass **Category 6A / Class EA Permanent Link** or **Channel** certification, as applicable, in accordance with **ANSI/TIA-568.2-D** and **ISO/IEC 11801** standards.

The bidder shall submit electronic and hard-copy certification reports for all tested links. Any link failing the certification shall be rectified and retested at no additional cost until it meets the specified standards.

### Wireless Network

- a. Coverage Verification
- b. Heat Map Validation
- c. Throughput Testing
- d. Roaming Test
- e. Latency Test
- f. Packet Loss Test
- g. Concurrent User Test

### Active Network

- a. Routing Validation
- b. Failover Testing
- c. Redundancy Testing
- d. QoS Validation
- e. Security Validation
- f. High Availability Testing
- g. Performance Benchmark Testing

Acceptance shall be carried out only after successful completion of all prescribed tests.

### 3.10 OEM Installation, Commissioning and Certification

The successful bidder shall ensure that the installation, configuration, integration, testing and commissioning of all **Active Network** Components, including but not limited to network security equipment, core switches, distribution switches, access switches, wireless controllers, wireless access points, network management system and associated software, are carried out by the respective bidder.

The bidder shall submit an **OEM Installation and Commissioning Certificate** confirming that the supplied active equipment has been installed, configured, integrated and commissioned in accordance with the OEM's prescribed standards, guidelines and best practices, and that the equipment is fully covered under the applicable OEM warranty and support.

For the **Passive Network Infrastructure**, the complete structured cabling system, including optical fiber backbone and copper cabling infrastructure, shall be installed by personnel certified or authorized by the respective Structured Cabling OEM. Upon completion of the work, the Structured Cabling OEM shall validate and certify the installation work and issue **Installation Certification**, confirming that:

- a. the complete passive infrastructure has been installed in accordance with the OEM's installation guidelines and industry standards;
- b. all copper and optical fiber links have successfully passed the prescribed certification tests;
- c. the complete structured cabling system qualifies for the OEM's application warranty for the period specified in the RFP; and

The tenderer reserves the right to seek verification of the submitted certificates directly from the respective OEM(s). Failure to furnish the required OEM installation and certification documents shall be treated as incomplete implementation, and the work shall not be considered for Final Acceptance until the same are submitted.

### 3.11 Documentation

The bidder shall submit:

- a. Approved Low Level Design
- b. As-Built Drawings
- c. Fiber Route Drawings
- d. Rack Layout Drawings
- e. Cable Schedule
- f. IP Addressing Scheme
- g. VLAN Details
- h. Wi-Fi Heat Maps
- i. OTDR Reports
- j. Fluke Test Reports

- k. Configuration Backup
- l. Asset Register
- m. Warranty Certificates
- n. License Details
- o. User Manuals
- p. Standard Operating Procedures
- q. Operation & Maintenance Manuals

Both soft copy and hard copy shall be submitted.

### 3.12 Training

The bidder shall conduct administrator-level training covering:

- a. Firewall Administration
- b. Switching
- c. Wireless Controller Administration
- d. Wi-Fi Management
- e. Network Management System
- f. Fault Diagnosis
- g. Backup and Restore
- h. Firmware Upgrade
- i. Preventive Maintenance
- j. Troubleshooting

Training shall include hands-on practical sessions.

### 3.13 General Requirements

The successful bidder shall execute the project on a **turnkey basis** and shall be responsible for the design, supply, delivery, installation, integration, configuration, testing, commissioning, documentation, training, warranty and support of the complete solution as specified in this RFP.

The bidder shall provide all hardware, software, licenses, subscriptions, accessories, cables, connectors, mounting hardware, consumables, interface modules, transceivers, patch cords, tools, equipment, services and any other items necessary for the successful installation, integration, testing, commissioning and operation of the complete solution, irrespective of whether such items are specifically identified in the Bill of Quantities (BOQ), provided they are required to meet the functional, technical, operational and performance requirements of this RFP for Wifi-7 Infrastructure. No additional payment shall be admissible on account of such items.

All products supplied under the contract shall be new, genuine, unused, of the latest available model of current year, free from manufacturing defects, and procured through the OEM or its authorized channel. The bidder shall furnish valid OEM authorization, warranty and support commitments, wherever applicable.

The bidder shall ensure that all materials, equipment, installation practices and workmanship conform to the applicable BIS, ISO/IEC, ANSI/TIA, IEEE, TEC and other relevant national/international standards, as well as the respective OEM recommendations and industry best practices.

The bidder shall coordinate with the Tenderer and all concerned agencies during project execution, obtain necessary work permits and approvals wherever required, ensure minimum disruption to existing services, maintain safety and security at the work site, protect existing infrastructure from damage, maintain proper housekeeping throughout the execution period, and restore all affected areas to their original condition upon completion of the work.

The bidder shall be solely responsible for the successful integration, interoperability, testing, commissioning and stabilization of the complete solution. The project shall be deemed complete only upon successful completion of all acceptance tests, submission of all required documentation, and formal acceptance by the Tenderer in accordance with the terms and conditions of the Contract.

The bidder shall deploy OEM-recommended security patches, firmware upgrades, hotfixes and critical software updates throughout the warranty period without any additional cost, after obtaining prior approval from the Tenderer.

### **3.14 Wireless Coverage Requirements**

The bidder shall carry out a comprehensive RF Site Survey, predictive wireless design and post-installation wireless validation to ensure that the deployed Wi-Fi infrastructure meets the coverage and performance requirements specified in the RFP.

The placement of the Access Points to achieve maximum performance and coverage has to be suggested by the OEM and the installation has to be done accordingly.

The bidder shall design the complete wireless infrastructure based on actual user density and application requirements. The proposed solution shall clearly indicate:

- Total supported users
- Concurrent users
- Peak concurrent users
- Devices per user
- Bandwidth estimation
- Traffic profile
- AP loading calculation
- Channel utilization

The bidder shall submit complete wireless capacity calculations along with Low Level Design.

During implementation, if any **wireless coverage gaps (dark spots)** are identified through the RF survey, site validation, or Acceptance Testing, the bidder shall optimize the wireless network by suitably reconfiguring, relocating or reorienting the Access Points, adjusting

antenna parameters (where applicable), and optimizing radio frequency settings without any additional cost to the Tenderer.

Where such optimization is insufficient to achieve the required coverage or performance, and additional Access Point(s) are technically justified, the bidder shall submit the RF survey findings and technical justification for approval by the Tenderer. Upon approval, the additional Access Point(s) shall be supplied, installed, configured, integrated, tested and commissioned at the **same unit rates and terms & conditions discovered under this RFP**, without any additional overheads, administrative charges or change in other contractual terms.

The requirement for additional Access Points shall be determined jointly by the Tenderer and the bidder based on the post-installation RF survey, heat map analysis and acceptance test results. The RF Survey shall be carried out using OEM-recommended or industry-standard wireless survey software and calibrated survey hardware. The survey shall include predictive and post-deployment validation and the bidder shall submit electronic survey project files along with the heat maps.

### **3.15 Log Retention (DoT / CERT-In Compliance)**

The proposed solution shall include adequate hardware, software, storage, licenses, and all associated infrastructure required for log retention in compliance with DoT, CERT-In, and other applicable statutory guidelines. No separate payment shall be made for the same.

All critical network and security components shall support centralized logging/Syslog, secure administrative access, role-based access control, time synchronization and audit trails.

Any cybersecurity incident, suspected compromise, unauthorized access or critical vulnerability affecting the supplied infrastructure shall be promptly reported to the Tenderer and necessary containment, investigation, remediation and restoration activities shall be carried out by the bidder without additional cost.

### **3.16 Data Privacy and Protection**

Where the proposed solution processes or stores user-related information, including mobile number, email address, authentication details, IP/MAC address, device information or access logs, the bidder shall ensure that such information is processed only for authorized purposes and protected against unauthorized access, disclosure, alteration or misuse.

The bidder/OEM and its authorized service providers, if any, shall comply with applicable data protection and privacy laws/rules and Tenderer's security policies. Access to such information shall be restricted to authorized personnel, and the data shall not be used, disclosed or transferred for any purpose unrelated to the Contract.

Upon expiry or termination of the Contract, such data shall be handed over and/or securely deleted, as instructed by the Tenderer and subject to applicable statutory retention requirements.

### **3.17 Network Performance Requirements**

The successful bidder shall design, implement, configure and optimize the complete wired and wireless network to achieve enterprise-grade performance suitable for high-density conference, exhibition and office environments. The network shall be designed considering user density, application requirements, mobility, redundancy and future scalability.

The bidder shall ensure that the deployed solution is capable of meeting the performance requirements specified in this RFP and shall demonstrate compliance during Performance Validation and Acceptance Testing.

### **3.18 Performance Validation & Acceptance Testing**

After completion of installation and configuration, the successful bidder shall carry out comprehensive performance validation jointly with the Tenderer. All testing shall be conducted using OEM-recommended or industry-standard testing tools and documented in the Acceptance Test Report.

The bidder shall submit the complete test methodology, tools to be used, test cases and expected results for approval before commencing the Acceptance Testing.

### **3.19 Product Lifecycle Compliance**

All proposed hardware, software, operating systems and licenses shall be current year manufactured, in production and fully supported by their respective OEMs on the date of bid submission. No product declared **End-of-Support (EOSL)** or equivalent by the OEM during the contract period.

During the entire warranty and Comprehensive Annual Maintenance Contract (CAMC) period, the OEM shall continue to provide software updates, security patches, bug fixes, technical assistance and hardware support for the proposed products.

In the event that any offered product is declared **End of support**, or equivalent by the OEM during the contract period, the successful bidder shall, without any additional cost to the Tenderer, supply, install, configure and commission an equivalent or higher model meeting or exceeding the original technical specifications and functional requirements, including migration of configuration, licenses (where transferable), and services, without any disruption to the existing network.

### **3.20 User Authentication, Guest Access & Captive Portal Requirements**

The proposed solution shall provide an integrated and centrally managed User Authentication, Guest Access and Captive Portal solution, integrated with the proposed NAC/AAA/RADIUS/WLC infrastructure, as applicable, with the following minimum requirements:

1. **Guest Authentication:** Support guest authentication through **SMS OTP, Email OTP WhatsApp-based authentication**, Token and QR Code base as applicable, with configurable authentication methods.
2. **Guest Registration & Lifecycle:** Provide self-registration for guest users and configurable user/session lifecycle management, including account creation, activation, expiry, logout and session termination.
3. **Captive Portal:** Provide a customizable captive portal supporting Government/MMCEC branding, logo, welcome message, Terms & Conditions/consent and configurable portal content.
4. **Access Control:** Support configurable user-based access policies, including VLAN/role assignment, Internet-only access, bandwidth limitation, session/idle timeout and concurrent-session control.
5. **Network Isolation:** Guest users shall be logically isolated from internal Government/administrative networks and shall be permitted access only to authorized services as per the configured security policy.
6. **Integration:** The solution shall integrate with the proposed **NAC/AAA/RADIUS, WLC and NMS** for authentication, authorization, policy enforcement, monitoring and centralized management.
7. **Logging & Audit:** The solution shall maintain appropriate authentication and session logs, including user identifier, authentication method, MAC/IP address, login/logout time, SSID/AP and session status, subject to applicable Government requirements.
8. **Availability:** Authentication and captive portal services shall support the proposed HA/resilient architecture and shall not create a single point of failure for guest access.
9. **Testing & Acceptance:** All configured authentication methods, captive portal functions, authorization policies, session timeout, guest isolation, logging and failure scenarios shall be demonstrated and successfully validated during FAT/Acceptance Testing.

The Successful Bidder shall provide all required platforms, software, licenses, subscriptions, APIs, gateways and third-party service integrations necessary for SMS OTP, Email OTP and WhatsApp-based authentication. The required subscription/usage entitlement shall be sufficient to cater to the user capacity designed under the proposed solution, including the anticipated concurrent and cumulative guest-user load. All such costs, including setup, configuration, integration, subscription, renewal and support for the entire contract period, shall be included in the bidder's quoted price. The bidder shall clearly specify the applicable usage entitlement/limits and any charges applicable beyond the included entitlement.

### **3.21 Capacity, Scalability and Licensing Validation**

The bidder shall ensure that the complete solution, including Core/Distribution/Access infrastructure, Firewall, Wireless LAN Controller, Wi-Fi Access Points, NAC/AAA, Captive Portal and NMS/Management platform, is adequately sized and licensed for the user/device capacity, traffic load and scalability requirements specified in the RFP.

The bidder shall submit a solution sizing statement along with the technical proposal clearly indicating supported capacity, proposed licensed capacity and scalability of the offered solution.

Any hardware, software, license or subscription required to achieve the specified capacity and functionality shall be deemed included in the quoted price and no additional cost will be paid by the GoG.

### **3.22 License and Subscription Continuity**

All hardware/software licenses, feature licenses, subscriptions, security services, management licenses and OEM support required for compliance with the RFP shall remain valid and operational throughout the applicable Contract/Warranty/O&M period.

There shall be no degradation, disabling or restriction of any mandatory RFP functionality due to expiry of licenses or subscriptions during the Contract period.

Renewal of all required licenses/subscriptions, including those related to Firewall security services, WLC/Wireless Management, NAC, NMS/SDN, Captive Portal/Authentication and associated management/analytics functionality, shall be the responsibility of the bidder and shall be included in the quoted Contract price.

### **3.23 Training and Knowledge Transfer**

The successful bidder shall provide adequate hands-on training and knowledge transfer to the officials/technical personnel nominated by the Tenderer covering operation, administration, monitoring, configuration, troubleshooting, security management, backup/restore and routine maintenance of the complete solution.

The bidder shall provide relevant training material, administration guides, configuration documents and troubleshooting procedures. Completion of training and knowledge transfer shall form part of the project acceptance/documentation requirements.

### **3.24 Exit Management – Data and Configuration Handover**

In addition to the Exit Management requirements specified elsewhere in the RFP, upon expiry or termination of the Contract, the bidder shall hand over the latest configurations, configuration backups, licenses, administrative information, network documentation, asset inventory, logs/reports and other project-related information required for continued operation of the infrastructure.

Where any Tenderer-related configuration, user information, logs or other project data is hosted or retained on bidder/OEM/cloud systems, the same shall be securely transferred and/or deleted as instructed by the Tenderer, subject to applicable statutory retention requirements. The bidder shall provide confirmation of such handover/deletion, wherever required.

### **3.25 Tools, Equipment, Man lift and Work-at-Height**

The Successful Bidder shall arrange, at its own cost, all tools, tackles, testing equipment, ladders, scaffolding, man lifts/boom lifts, lifting equipment, safety equipment and skilled manpower required for installation, cabling, AP mounting, testing, commissioning and maintenance activities, including work at height.

The Successful Bidder shall comply with all applicable statutory safety requirements and provide necessary PPE, safety harnesses, helmets and other protective equipment to its personnel. The Successful Bidder shall maintain adequate Employees' Compensation/Workmen Compensation, personal accident, third-party liability and other applicable insurance coverage for its personnel, equipment and activities throughout the execution and maintenance period.

The Successful Bidder shall be solely responsible for any accident, injury, disability, loss of life, damage to property or third-party claim arising out of or in connection with its activities, personnel, subcontractors, tools or equipment, except to the extent directly attributable to the Tenderer. The Successful Bidder shall indemnify and keep the Tenderer harmless against all related claims, liabilities, damages, penalties and expenses.

All costs towards safety measures, insurance, deployment, transportation, operation and removal of equipment and manpower shall be deemed included in the quoted price, and no additional payment shall be admissible on this account.

---

## *Section 4*

### *Final Acceptance Testing (FAT) & Go-Live*

---

## 4.1 General

The Acceptance Testing shall be carried out after successful installation, integration and commissioning of the complete solution. The bidder shall submit a detailed Acceptance Test Plan (ATP), including test methodology, test procedures, test tools, expected results and acceptance criteria, for approval by the Tenderer prior to commencement of Acceptance Testing.

The Acceptance Testing shall include, but not be limited to, the following activities:

## 4.2 Scope of Acceptance Testing

The Acceptance Testing shall be conducted after successful completion of supply, installation, configuration, integration and commissioning of the complete solution.

The Successful Bidder shall prepare and submit a comprehensive **Acceptance Test Plan (ATP)**, detailing the test methodology, test procedures, tools, prerequisites, expected results and acceptance criteria for approval by the Tenderer before commencement of Acceptance Testing.

Acceptance Testing shall include, but not be limited to, the following activities.

### 4.2.1 Passive Infrastructure Testing

The bidder shall carry out complete testing of the passive network infrastructure including:

- a. 100% Fluke DSX Certification of all copper structured cabling links.
- b. 100% OTDR testing of all Optical Fibre links.
- c. 100% Optical Loss Testing (OLTS)/Power Meter testing.
- d. Verification of fibre splicing quality.
- e. Verification of splice loss.
- f. Verification of cable routing.
- g. Verification of cable labelling.
- h. Verification of cable termination.
- i. Verification that the passive infrastructure complies with applicable TIA/EIA, ISO/IEC and OEM standards.
- j. Submission of complete electronic test reports.

## **4.2.2 Active Network Equipment Testing**

The bidder shall verify proper installation and operation of all active network components including:

- a. Firewall
- b. Core Switches
- c. Distribution Switches
- d. Access Switches
- e. Wireless LAN Controllers
- f. Wi-Fi 7 Access Points
- g. Network Management System
- h. Authentication/Captive Portal Solution

The testing shall include:

- Hardware health verification
- Software/Firmware verification
- License verification
- Configuration verification
- High Availability verification
- VLAN verification
- Inter-VLAN Routing
- Link Aggregation
- QoS verification
- DHCP Relay
- NTP synchronization
- CPU & Memory utilization
- Power Supply redundancy
- Uplink redundancy

## **4.2.3 Functional Testing**

The bidder shall demonstrate successful operation of:

- End-to-End connectivity
- Internet access
- LAN access
- User Authentication
- Captive Portal

- SMS OTP
- Email OTP
- WhatsApp Authentication
- User Authorization
- Network Management
- Logging
- Monitoring
- Policy Enforcement

#### **4.2.4 Wireless Network Testing**

Wireless acceptance testing shall include:

- a. Verification of Wi-Fi 7 features supported by the proposed solution.
- b. Post-installation RF Survey using OEM-recommended or industry-standard RF Survey tool.
- c. Verification of RF coverage against the approved RF Design.
- d. Detection and rectification of wireless coverage dark spots within designated service areas.
- e. Verification of SSID functionality.
- f. Verification of WPA3 Enterprise Authentication.
- g. Verification of Guest Access.
- h. Verification of Captive Portal.
- i. Verification of Client Roaming.
- j. Verification of Channel Assignment.
- k. Verification of Automatic Power Optimization.
- l. Concurrent Client Connectivity Testing.
- m. Wireless Throughput Validation.
- n. Wireless Controller Failover.
- o. AP Registration Verification.

The bidder shall submit:

- RF Survey Report

- RF Heat Maps
- Coverage Maps
- Channel Plan
- Power Plan

## **4.2.5 Performance Validation**

The bidder shall demonstrate the performance of the complete network under representative operating conditions.

Performance validation shall include:

- Wired Network Throughput
- Wireless Network Throughput
- Concurrent Client Connectivity
- Internet Browsing
- Video Streaming
- Voice over Wi-Fi (if applicable)
- DHCP Allocation
- DNS Resolution
- Failover Recovery
- Network Stability

Performance testing shall be carried out using industry-standard traffic generation and network testing tools.

The bidder shall demonstrate network performance under representative concurrent user load as per the approved network design under the representative concurrent user load defined in the approved High Level Design (HLD) and Low Level Design (LLD).

## **4.2.6 Security Testing**

Security validation shall include:

- Firewall Policies
- NAT
- User Authentication
- Role Based Access Control

- Administrative Access
- Password Policies
- Logging
- Audit Trail
- Secure Remote Access
- Digital Certificates
- Security Event Monitoring
- High Availability of Security Appliances

### **4.2.7 High Availability & Failover Testing**

The bidder shall demonstrate High Availability by simulating failure of each redundant component individually.

The testing shall include:

- Core Switch Failover
- Firewall Failover
- Wireless Controller Failover
- Power Supply Failure
- Uplink Failure
- Link Redundancy
- Internet Link Failover (where applicable)

Failure of a single hardware device shall not result in complete loss of network services.

### **4.2.8 Network Management & Monitoring**

Verification shall include:

- Device Discovery
- Inventory Management
- Alarm Generation
- Event Monitoring
- Dashboard
- Historical Reports
- Performance Monitoring
- Configuration Backup
- Configuration Restore
- Syslog Integration
- SNMP Monitoring
- User Role Management

### **4.2.9 Documentation Verification**

The bidder shall submit:

- As-built Drawings
- High Level Design (HLD)
- Low Level Design (LLD)
- Rack Layout
- Cable Layout
- Port Mapping
- IP Address Plan
- VLAN Matrix
- RF Heat Maps
- Channel Plan
- Asset Register
- License Register
- Configuration Backup
- Operation & Maintenance Manual
- Preventive Maintenance Checklist
- Training Report

#### **4.2.10 OEM Documentation**

The bidder shall submit:

- OEM Installation Certificate
- OEM Commissioning Certificate
- OEM Warranty Certificate
- OEM License Certificate
- OEM Support Registration
- OEM Product Lifecycle Declaration confirming that all supplied products are current, factory-new and not End-of-Sale (EOS), End-of-Life (EOL) or End-of-Support (EOSL) as on the bid submission date.

#### **4.2.11 Defect Rectification**

Any defect, deficiency or non-conformity observed during Acceptance Testing shall be rectified by the Successful Bidder at no additional cost to the Tenderer.

The affected tests shall be repeated until successful completion.

No component shall be accepted unless it successfully passes the applicable Acceptance Tests.

### **4.3 Final Acceptance**

The project shall be considered to have achieved Final Acceptance only after:

- a. Successful completion of all Acceptance Tests.

- b. Successful completion of all Performance Validation Tests.
- c. Successful completion of all Security Tests.
- d. Successful completion of all High Availability Tests.
- e. Submission and acceptance of all documentation.
- f. Submission of all OEM Certificates.
- g. Resolution of all observations.
- h. Stable operation of the complete solution for **07 consecutive calendar days** after commissioning without any Severity-1 incident attributable to the deployed solution.
- i. Issuance of Final Acceptance Certificate (FAC) by the Tenderer.

**Annexure-X : Acceptance Test Matrix**

| Test ID  | Component      | Test Case           | Test Method             | Acceptance Criteria        |
|----------|----------------|---------------------|-------------------------|----------------------------|
| PASS-001 | Copper Cabling | Fluke Test          | Fluke DSX               | 100% PASS                  |
| PASS-002 | OFC            | OTDR                | OTDR Report             | 100% PASS                  |
| PASS-003 | OFC            | OLTS                | Power Meter             | Within OEM Limits          |
| CORE-001 | Core Switch    | Installation        | Physical Verification   | Installed                  |
| CORE-002 | Core Switch    | Redundant PSU       | Remove One PSU          | No Service Impact          |
| CORE-003 | Core Switch    | HA Failover         | Shutdown Primary        | Traffic Continues          |
| CORE-004 | Core Switch    | VLAN                | Connectivity Test       | Successful                 |
| CORE-005 | Core Switch    | Inter-VLAN Routing  | Ping Test               | Successful                 |
| CORE-006 | Core Switch    | LACP                | Disable One Link        | Traffic Continues          |
| FW-001   | Firewall       | HA                  | Shutdown Primary        | Automatic Failover         |
| FW-002   | Firewall       | Security Policy     | Test Traffic            | Policy Enforced            |
| FW-003   | Firewall       | NAT                 | Internet Access         | Successful                 |
| WLAN-001 | Wi-Fi 7 AP     | AP Registration     | Controller Verification | 100% AP Registered         |
| WLAN-002 | Wi-Fi 7 AP     | SSID Broadcast      | Client Test             | Successful                 |
| WLAN-003 | Wi-Fi 7 AP     | WPA3 Authentication | Login Test              | Successful                 |
| WLAN-004 | Wi-Fi 7 AP     | Guest Portal        | OTP Login               | Successful                 |
| WLAN-005 | Wi-Fi 7 AP     | Roaming             | Continuous Walk Test    | Seamless Roaming (No Drop) |

|          |               |                       |                   |                           |
|----------|---------------|-----------------------|-------------------|---------------------------|
| WLAN-006 | Wi-Fi 7 AP    | RF Coverage           | RF Survey         | As per Approved RF Design |
| WLAN-007 | Wi-Fi 7 AP    | Concurrent Clients    | Multi-client Test | Stable Operation          |
| WLAN-008 | Wi-Fi 7 AP    | Throughput            | Traffic Generator | As per Approved Design    |
| NMS-001  | NMS           | Device Discovery      | Auto Discovery    | 100% Devices Visible      |
| NMS-002  | NMS           | Alarm                 | Interface Down    | Alarm Generated           |
| DOC-001  | Documentation | As-built Drawings     | Document Review   | Submitted                 |
| DOC-002  | Documentation | Asset Register        | Verification      | Submitted                 |
| OEM-001  | OEM           | Warranty Certificate  | Document Review   | Submitted                 |
| OEM-002  | OEM           | Lifecycle Declaration | OEM Letter        | Submitted                 |

The Successful Bidder shall arrange, at its own cost, all test equipment, software tools, temporary licenses, traffic generators, test clients and skilled manpower required for Acceptance Testing.

## 4.4 Go-Live

Following successful Final Acceptance, the bidder shall assist the Tenderer in placing the complete solution into production (Go-Live).

The Go-Live activities shall include:

- Migration from the existing network (where applicable).

The bidder shall provide onsite technical support during the Go-Live period and shall continuously monitor the solution to ensure stable and uninterrupted operation.

---

## *Section 5*

### *Delivery Milestones*

---

| <b>Milestone</b> | <b>Deliverable</b>                                                                                                                                                                                                                           | <b>Timeline</b>                   | <b>Penalty</b>                                                                                                                                                                                                                 |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>1</b>         | Submission of Performance Bank Guarantee (PBG), Project Kick-off Meeting, Project Plan, Resource Deployment Plan and Detailed Implementation Schedule                                                                                        | <b>T + 07 Calendar Days</b>       | In case of non-submission of the Performance Bank Guarantee (PBG) within the stipulated timeline, the Earnest Money Deposit (EMD) shall be forfeited, and the Tenderer reserves the right to cancel the award of the Contract. |
| <b>2</b>         | Site Survey, RF Survey, Detailed Network Design, Bill of Material Validation and Approval                                                                                                                                                    | <b>T1 = T + 10 Calendar Days</b>  | A penalty of <b>0.5% per week or part thereof proportionately</b> of the delayed component shall be levied for delay beyond the stipulated timeline, subject to a maximum of <b>10% of the TCV</b> .                           |
| <b>3</b>         | Delivery of all Hardware, Software, Licenses, Passive Components and other materials at the designated location(s) of the Tenderer / Vendor Warehouse                                                                                        | <b>T2 = T + 30 Calendar Days</b>  | A penalty of <b>0.15% per week or part thereof proportionately</b> of the delayed component shall be levied for delay beyond the stipulated timeline, subject to a maximum of <b>10% of the TCV</b> .                          |
| <b>4</b>         | Completion of Passive Infrastructure comprising OFC, Structured Cabling, Racks, Conduits, Civil Works, Mounting Structures, Termination, Labelling, Testing and Certification                                                                | <b>T3 = T2 + 15 Calendar Days</b> | A penalty of <b>0.15% per week or part thereof proportionately</b> of the delayed component shall be levied for delay beyond the stipulated timeline, subject to a maximum of <b>10% of the TCV</b>                            |
| <b>5</b>         | Installation, Configuration, Integration and Commissioning of Active Network Components including Firewall, Core Switches, Distribution Switches, Access Switches, Wireless Controllers, Access Points, NMS and associated software/licences | <b>T4 = T2 + 15 Calendar Days</b> | A penalty of <b>0.15% per week or part thereof proportionately</b> of the delayed component shall be levied for delay beyond the stipulated timeline, subject to a maximum of <b>10% of the TCV</b>                            |

|          |                                                                                                                                |                                   |                                                                                                                                                                         |
|----------|--------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>6</b> | Final Acceptance Testing (FAT), Validation, Documentation, OEM Certification and Go-Live of the Complete Wi-Fi Infrastructure. | <b>T5 = T4 + 05 Calendar Days</b> | A penalty of <b>0.15% per week or part thereof</b> of the TCV shall be levied for delay beyond the stipulated timeline, subject to a maximum of <b>10% of the TCV</b> . |
|----------|--------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**Notes:**

1. **T** = Date of issuance of the Contract / Work Order.
2. The bidder shall deploy adequate manpower, tools and resources to adhere to the above implementation schedule.
3. If the selected bidder fails to supply or install any ordered item for reasons attributable to the bidder, the bidder shall be liable to compensate the Tenderer for the differential procurement cost, if any, in addition to the forfeiture or invocation of the applicable Performance Security, as per the terms of the Contract.
4. The above implementation and delivery penalties are independent of and in addition to the Service Level Agreement (SLA) penalties applicable during the Warranty/Operation & Maintenance period.
5. Installation and commissioning shall be carried out in close coordination with the Tenderer to minimise disruption to existing network services.
6. Final Acceptance Testing (FAT) shall be conducted only after successful completion of installation, integration, configuration, testing and submission of all mandatory documentation, certifications and OEM warranties.
7. The Tenderer may permit implementation at multiple sites in parallel. However, such parallel execution shall not entitle the bidder to any extension of the overall project completion timeline.
8. Notwithstanding the penalty specified against each individual Milestone above, the cumulative delay penalty recoverable under all Milestones (2 to 6) combined shall not exceed 10% of the Total Contract Value (TCV). Penalties under different Milestones shall be computed independently but shall be subject to this overall cap.

---

## *Section 6*

### *Service Level Agreement (SLA) and Payment Schedule*

---

## 6.1 General

The successful bidder shall ensure that the complete Wi-Fi infrastructure, including active and passive components, software, licenses and associated services, performs in accordance with the requirements specified in this RFP throughout the warranty and support period.

The bidder shall provide comprehensive onsite support, preventive maintenance, corrective maintenance, firmware/software updates, security patches and replacement of defective hardware during the warranty period without any additional cost to the Tenderer.

## 6.2 Service Availability

Availability shall be measured excluding approved maintenance windows.

## 6.3 Incident Classification

Incidents shall be classified into the following severity levels based on their impact on the network, users and business operations.

| Severity                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Priority-1<br/>(P1) – Critical</b> | Any security breach, Complete outage of a critical network service or infrastructure affecting the entire campus or a major operational area, with no acceptable workaround available. This includes failure of critical network components (e.g., Firewall, Core Switch, Wireless Controller), complete network outage, security incidents impacting network operations, or simultaneous failure of <b>more than 25% of the deployed Access Points</b> due to a common cause. Immediate attention is required. Any outage during Honourable PM/CM Events shall be considered under this severity. |
| <b>Priority-2<br/>(P2) – Major</b>    | Partial degradation of services affecting block, floor, multiple access switches or a significant number of users. This includes failure of critical network components affecting a specific area, or simultaneous failure of <b>5% to 25% of the deployed Access Points</b> or all Access Points within a building/floor/zone. A limited workaround may exist, but normal operations are affected.                                                                                                                                                                                                |
| <b>Priority-3<br/>(P3) – Minor</b>    | Localized issue affecting a limited number of users or a specific area with an available workaround. This includes failure of <b>less than 5% of the deployed Access Points</b> , failure of a single Access Point, isolated network ports, or localized coverage/performance issues not significantly impacting overall operations.                                                                                                                                                                                                                                                               |

|                                                            |                                                                                                                                                                            |
|------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                            |                                                                                                                                                                            |
| <b>Priority-4<br/>(P4) – Low /<br/>Service<br/>Request</b> | Non-service-impacting issues, cosmetic defects, planned configuration changes, information requests, or enhancement requests that do not affect normal network operations. |

## 6.4 Response and Resolution Time

| Severity | Response Time | Resolution Time |
|----------|---------------|-----------------|
| P1       | 15 Minutes    | 30 Minutes      |
| P2       | 30 Minutes    | 2 Hours         |
| P3       | 30 Minutes    | 4 Hours         |
| P4       | 30 Minutes    | 8 Hours         |

## 6.5 Penalties

### 6.5.1 Delay in Project Implementation

Delay in achieving any implementation milestone shall attract penalties as specified under the "Delivery Milestones" section of this RFP.

## 6.5.2 SLA Penalties

| Sr. No. | SLA Parameter                                                                                                           | SLA Requirement      | Measurement & Applicability                                                                                                                                                           | Penalty Calculation                                                                         | Maximum Penalty                    |
|---------|-------------------------------------------------------------------------------------------------------------------------|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|------------------------------------|
| 1       | Core Network Infrastructure Availability (Firewall, Core Switches, Wireless Controllers, NMS, Distribution Switch, NAC) | ≥ 99.95% per quarter | Availability shall be measured per device category and aggregated quarterly across all Core Network Infrastructure. Scheduled maintenance approved by the Tenderer shall be excluded. | <b>10 % of the Quarterly Payment</b> for every <b>0.10% shortfall</b> below the SLA target. | Up to <b>10% of QP</b> per quarter |
| 2       | Access Switch Availability                                                                                              | ≥ 99.90% per quarter | Availability shall be measured across all Distribution and Access Switches and aggregated quarterly.                                                                                  | <b>1% of the Quarterly Payment</b> for every <b>0.10% shortfall</b> below the SLA target.   | Up to 10% of QP per quarter        |
| 3       | Wi-Fi Access Point Availability                                                                                         | ≥ 99.50% per quarter | Availability shall be measured across all deployed Access Points and aggregated quarterly. Planned maintenance shall be excluded.                                                     | <b>1% of the Quarterly Payment</b> for every <b>0.10% shortfall</b> below the SLA target.   | Up to 10% of QP per quarter        |
| 4       | Priority-1 (P1) Incident Resolution Time                                                                                | ≤ 30 Minute          | Measured per incident from the time of incident logging in the Helpdesk/Ticketing System until                                                                                        | <b>Forfeit of PBG.</b>                                                                      | -----                              |

|   |                                                                                                           |                                                                             |                                                   |                                                                                                      |                            |
|---|-----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|---------------------------------------------------|------------------------------------------------------------------------------------------------------|----------------------------|
|   |                                                                                                           |                                                                             | restoration of service.                           |                                                                                                      |                            |
| 5 | Priority-2 (P2) Incident Resolution Time                                                                  | ≤ 2 Hours                                                                   | Measured per incident.                            | <b>05% of the Quarterly Payment</b> per incident breach, aggregated quarterly.                       | Up to 5% of QP per quarter |
| 6 | Priority-3 (P3) Incident Resolution Time                                                                  | ≤ 4 Hours                                                                   | Measured per incident.                            | <b>01% of the Quarterly Payment P</b> per incident breach, aggregated quarterly.                     | Up to 5% of QP per quarter |
| 7 | Priority-4 (P4) Incident Resolution Time / Service Request                                                | ≤ 8 Hours                                                                   | Measured per incident.                            | <b>0.10% of the Quarterly Payment</b> per incident breach, aggregated quarterly.                     | Up to 2% of QP per quarter |
| 8 | Submission of Quarterly Preventive Maintenance (PM) Report, SLA Compliance Report and Health Check Report | As specified in the RFP                                                     | Measured per instance of delay or non-submission. | <b>0.10% of the Quarterly Payment</b> per instance.                                                  | -----                      |
| 9 | Resident O&M Manpower Availability                                                                        | 100% deployment of minimum resident manpower throughout the Warranty period | Measured quarterly                                | <b>Pro-rata deduction from quarterly manpower payment for the actual period of non-availability.</b> | As per actual              |

The cumulative SLA penalties (comprising Availability SLA penalties, Incident Resolution SLA penalties, and Reporting SLA penalties) levied in any quarter shall not exceed 25% of the Quarterly Payment (QP), irrespective of the number of individual SLA parameters breached. The per-parameter maximum penalties specified in above Table shall apply as sub-limits within this overall ceiling of 25% of QP.

**Notes:**

1. **QP (Quarterly Payment)** means the quarterly payment payable to the bidder during the Warranty/Support period.
2. Availability shall be calculated as: **Availability (%) = [(Total Time – Downtime) / Total Time] × 100.**
3. All penalties shall be deducted from the applicable Quarterly Payment. Where the recoverable penalty exceeds the Quarterly Payment, the balance shall be recovered from subsequent payments and/or the Performance Bank Guarantee (PBG).
4. Repeated occurrence of the same incident due to failure to permanently rectify the root cause may be treated as separate incidents for SLA evaluation.
5. Levy of SLA penalties shall not relieve the bidder of its contractual obligations or restrict the Tenderer's right to invoke any other remedies available under the Contract.
6. Availability SLA penalties and Incident Resolution SLA penalties shall be calculated independently and may apply concurrently during the same quarter. However, where the same incident results in a breach of both the Availability SLA and the Incident Resolution SLA for the same device, component or service, only the higher of the two applicable penalties shall be levied for that incident. This exception shall not apply to separate or unrelated incidents occurring during the same quarter.
7. The following events shall be excluded from the calculation of Availability (Uptime) SLA, provided the bidder has promptly notified the Tenderer and maintained adequate supporting records:
  - a. Scheduled maintenance activities approved in advance by the Tenderer.
  - b. Power supply failures, electrical outages, DG/UPS failures, HVAC failures, or any other utility-related disruptions at the Tenderer's premises that are not attributable to the bidder.
  - c. Failure or outage of third-party infrastructure or services not under the bidder's scope of work, including ISP/Internet/MPLS connectivity, WAN links, leased circuits, or utility services.
  - d. Downtime arising due to force majeure events, including but not limited to natural calamities, floods, earthquakes, fire, riots, civil disturbances, acts of war, or any other event beyond the reasonable control of the bidder.
  - e. Downtime resulting from changes, maintenance activities, or instructions carried out by the Tenderer or any agency authorized by the Tenderer, without the involvement or fault of the bidder.

f. Downtime due to reasons directly attributable to the Tenderer, including denial of site access, delay in providing power, rack space, civil readiness, network dependencies, or any other prerequisite required for restoration of services.

g. Such exclusions shall be considered only where the bidder has reported the incident through the designated Helpdesk/Ticketing System and maintained complete evidence to substantiate the cause of downtime.

## 6.6 Repeated Failures

If any Critical Incident occurs repeatedly due to the same unresolved root cause on more than three occasions within a calendar month, the Tenderer may require replacement of the defective hardware or corrective action at no additional cost.

## 6.7 Non-Compliance

Repeated failure to meet contractual obligations, excessive SLA violations, and abandonment of work or failure to provide support may be treated as breach of contract and may result in invocation of Performance Security, termination of the Contract, risk purchase or any other action deemed appropriate by the Tenderer.

## 6.8 Payment Terms

Payment shall be released only after successful completion of the respective milestones and submission of all supporting documents.

| Milestone | Milestone Description                                                                                                                                                                     | Payment                                                                                                                                                                                                                       |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| M1        | Supply and delivery of Hardware, Software, Licenses, Passive Components and all other materials at the designated location(s) of the Tenderer/bidder's warehouse at Ahmedabad/Gandhinagar | <b>30% of the delivered component. Payment under M1 shall be released only after successful inspection, physical verification and acceptance of the delivered materials by the Tenderer or its authorized representative.</b> |
| M2        | Completion of installation, configuration, integration, testing, commissioning of the passive infrastructure with submission of all mandatory test reports (Fluke DSX, OTDR, OLTS).       | <b>20% of the commissioned Infrastructure. Payment under M2 shall be released only after completion of passive infrastructure work with mandatory test report.</b>                                                            |

|           |                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                 |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>M3</b> | Completion of installation, configuration, integration, testing, commissioning, Final Acceptance Testing (FAT), submission of all mandatory test reports (Fluke DSX, OTDR, OLTS), OEM certificates, documentation and successful Go-Live of the complete Wi-Fi Infrastructure.  | <b>40% of the Total Contract Value Payment under M3 shall be released only after issuance of the Final Acceptance Certificate (FAC) by the Tenderer.</b>                                                        |
| <b>M4</b> | Operation & Maintenance including preventive maintenance, corrective maintenance, firmware/software updates, security patches, hardware replacement, SLA compliance, and technical support for a period of <b>Five (5) years</b> from the date of issuance of the Go Live date. | <b>10% of the Total Contract Value, payable in 20 equal quarterly instalments over Five (5) years, subject to satisfactory SLA compliance..</b>                                                                 |
| <b>M5</b> | Payment of Resident O&M Manpower                                                                                                                                                                                                                                                | Payment towards the Manpower Category-C shall be released in equal quarterly instalments over the five (5) year period, subject to: Deployment of the prescribed manpower.<br>Submission of attendance records. |

The bidder shall submit the following documents along with the invoice whichever is applicable.

- a. Delivery Challans.
- b. Inspection Report.
- c. Installation Report.
- d. FAT Report.
- e. Go-Live Certificate.
- f. Final Acceptance Certificate.
- g. OEM Warranty Certificates.
- h. OEM Installation & Commissioning Certificates.
- i. 25-Year OEM Application Warranty Certificate for Passive Cabling.
- j. Asset Register.

- k. As-built Drawings.
- l. Test Reports (Fluke DSX, OTDR and OLTS).
- m. Any other documents required by the Tenderer.

## 6.9 General Payment & Billing Conditions

### 1. Quarterly Payments

Payments towards the Milestone M4 shall be released at the end of each quarter over a period of **Five (5) years** from the date of issuance of the Go Live, subject to satisfactory SLA compliance and fulfilment of the conditions specified in the Contract.

### 2. Invoice Submission

The bidder shall submit the applicable invoice along with all supporting documents, preventive maintenance reports, SLA compliance reports, health check reports and any other documents specified in the RFP for processing of payments.

### 3. Supporting Documentation

The bidder shall submit all relevant documents, including but not limited to inspection reports, installation reports, Fluke DSX test reports, OTDR and OLTS reports, RF validation reports, OEM warranty certificates, OEM installation and commissioning certificates, as-built drawings, asset register, configuration backups and any other documents required by the Tenderer for verification of work completed.

### 4. Verification and Certification

All payments shall be subject to verification and certification by the Tenderer or its designated representative that the corresponding milestone has been successfully completed in accordance with the provisions of the Contract.

### 5. Deduction of Penalties and Statutory Taxes

The Tenderer shall be entitled to deduct applicable implementation delay penalties, SLA penalties and any other recoverable dues from the payments payable to the bidder. The Tenderer shall also deduct TDS and other statutory deductions as applicable under prevailing laws.

### 6. Recovery of Excess Penalties

where the applicable penalties exceed the amount payable under any milestone or quarterly warranty payment, the balance amount shall be recovered from subsequent payments, the Performance Bank Guarantee (PBG), or any other amount payable to the bidder under the Contract.

### 7. Final Acceptance Certificate (FAC)

Following successful completion of Acceptance Testing, the bidder shall assist the Tenderer in placing the complete solution into production (Go-Live).

### 8. Commencement of Warranty Period

The Warranty and SLA period shall commence from the date of issuance of the Go Live of the project.

### 9. Go-Live Declaration

Go-Live shall be declared only after successful completion of all FAT activities, coverage validation, submission of all mandatory test reports, successful integration of all active and passive infrastructure, resolution of all critical observations and formal certification by the Tenderer.

10.

**11. Final Payment Conditions**

Release of payment under Milestone M3 shall be subject to successful completion of FAT, Go-Live of the project. Release of quarterly payments under Milestone M4 shall be subject to successful completion of knowledge transfer, submission of all as-built documents, configuration backups, passwords (through a secure mechanism), licenses, and formal project closure and continued compliance with the Service Level Agreements throughout the Warranty period

**12. No Deemed Acceptance**

Mere supply, installation or commissioning of equipment shall not constitute acceptance of the project. Payments shall be governed strictly by successful completion of the respective milestone and certification by the Tenderer.

**13. No Interest on Delayed Payments**

No interest shall be payable by the Tenderer on any payment withheld or delayed due to incomplete work, pending documentation, non-compliance with contractual obligations, or unresolved observations attributable to the bidder.

---

## *SECTION 7*

### *Comprehensive Warranty & Operations and Maintenance (O&M) Period*

---

## 7.1 General

The successful bidder shall provide comprehensive Operations & Maintenance (O&M) support for the complete Wi-Fi Infrastructure for a period of **Five (5) years** from the date of issuance of the Final Acceptance Certificate (FAC).

The O&M services shall include preventive maintenance, corrective maintenance, fault diagnosis, hardware replacement, software support, firmware upgrades, security updates, configuration management, performance optimization, incident management, reporting, and technical support for all active and passive components supplied under this Contract.

The bidder shall be fully responsible for ensuring uninterrupted, reliable and secure operation of the complete network infrastructure throughout the Warranty period.

## 7.2 Scope of O&M

The bidder shall undertake, but not be limited to, the following activities:

### A. Active Network Infrastructure

The bidder shall operate and maintain:

- Firewall
- Core Switches
- Distribution Switches
- Access Switches
- Wireless Controllers
- Wi-Fi 7 Access Points
- Network Management System (NMS)
- Transceivers (SFP/SFP+/SFP28/QSFP)
- Software and Licenses
- All associated accessories supplied under the Contract.

### B. Passive Infrastructure

The bidder shall maintain:

- Optical Fibre Cable (OFC)
- Structured Cabling (Cat6A)
- LIUs
- Patch Panels
- Patch Cords

- Keystone Jacks
- Faceplates
- Racks
- HDPE Pipes
- PVC Conduits
- Outdoor Enclosures
- Mounting Hardware
- Earthing and Cable Management

## 7.3 Corrective Maintenance

The bidder shall:

- Attend all complaints within the SLA.
- Diagnose hardware and software faults.
- Restore services within prescribed SLA timelines.
- Replace defective hardware.
- Replace damaged accessories.
- Repair passive cabling wherever required.
- Restore complete functionality without additional cost.

Temporary workarounds shall not be considered permanent resolution.

## 7.4 Preventive Maintenance

Preventive Maintenance shall be carried out **at least once every six (6) months**, or more frequently if recommended by the OEM.

Preventive Maintenance shall include:

- Physical inspection of all equipment.
- Cleaning of racks and equipment.
- Verification of power supplies.
- Fan health verification.
- Temperature monitoring.
- PSU health verification.
- Optical power verification.
- Cable dressing inspection.
- Patch panel inspection.
- Fibre termination inspection.
- Verification of earthing.
- AP mounting inspection.
- Cable route inspection.
- Rack locking mechanism verification.
- Firmware review.
- Security patch review.

- Backup verification.
- Configuration verification.
- Log verification.
- Alarm verification.
- Performance review.
- RF optimization.
- Channel utilization review.
- Transmit power optimization.
- Detection and removal of rogue Access Points.
- Verification of SSID functionality.
- Validation of WPA3 security configuration.

A Preventive Maintenance Report shall be submitted after every maintenance cycle.

## **7.5 Firmware, Software and Security Updates**

The bidder shall:

- Install OEM-recommended firmware upgrades.
- Apply security patches.
- Install software updates.
- Deploy hotfixes.
- Resolve software bugs.
- Upgrade device signatures where applicable.
- Maintain supported software releases.

All upgrades shall be carried out after obtaining approval from the Tenderer.

## **7.6 Configuration Management**

The bidder shall:

- Maintain current configurations.
- Maintain version control.
- Maintain configuration backups.
- Restore configurations whenever required.
- Record every configuration change.

No configuration shall be changed without approval of the Tenderer.

## **7.7 Incident Management**

The bidder shall:

- Log every incident.
- Classify incidents as P1/P2/P3/P4.

- Provide ticket number.
- Provide ETA.
- Restore services.
- Close tickets only after confirmation from the Tenderer.
- Maintain complete incident history.

## 7.8 Root Cause Analysis (RCA)

For every Priority-1 and Priority-2 incident, the bidder shall submit an RCA Report containing:

- Incident description.
- Timeline.
- Root cause.
- Corrective actions.
- Preventive actions.
- Recommendations.

The RCA Report shall be submitted within:

- **P1 Incident:** 1 Working Days.
- **P2 Incident:** 2 Working Days.

## 7.9 Spare Inventory

The bidder shall maintain adequate onsite/offsite spare inventory throughout the warranty period to meet SLA requirements

The bidder shall ensure availability of critical spares including but not limited to:

- Access Switches
- Wi-Fi Access Points
- SFP Modules
- Patch Cords
- Patch Panels
- Fibre Accessories

Non-availability of spares shall not be accepted as a reason for SLA non-compliance.

## 7.10 Performance Optimization

The bidder shall periodically optimize:

- Coverage, signal strength
- Channel allocation
- Transmit power
- Client load balancing

- Roaming performance
- QoS policies
- Network utilization
- Bandwidth utilization
- Firewall performance
- Switch performance

Any wireless dark spots identified during the Warranty period shall be investigated and optimized through configuration changes, RF tuning, relocation or reorientation of Access Points without additional cost. Where additional Access Points are technically required, the procedure specified in this RFP shall apply.

## **7.11 Network Monitoring**

The bidder shall continuously monitor:

- Device availability.
- CPU utilization.
- Memory utilization.
- Link utilization.
- Interface errors.
- Temperature.
- Power supply health.
- Wireless health.
- Rogue AP detection.
- Client connectivity.
- Security events.

## **7.12 Reporting**

The bidder shall submit:

### **Monthly Reports**

- Incident Summary
- Device Health
- Uptime Report
- Network Utilization
- Security Events
- Firmware Status
- Inventory Changes

### **Quarterly Reports**

- SLA Compliance Report
- Preventive Maintenance Report
- Health Check Report

- Performance Analysis
- Capacity Planning Report
- Security Compliance Report
- Configuration Backup Verification Report

### **7.13 OEM Support**

The bidder shall ensure:

- Valid 24x7 OEM support throughout the Warranty period.
- Active software subscriptions.
- Technical Assistance Centre (TAC) support.
- Access to firmware, software updates and security patches.
- Continuity of OEM warranties.

### **7.14 Documentation**

The bidder shall maintain updated:

- Asset Register
- Network Topology
- IP Address Plan
- VLAN Details
- Rack Layout
- Port Mapping
- Configuration Backup
- RF Heat Maps
- Warranty Register
- License Register
- Change Log
- Incident Register

### **7.15 Replacement of Defective Equipment**

Any equipment declared defective shall be replaced with a new unit of equal or higher specifications without additional cost to the Tenderer.

The replacement equipment shall carry warranty for the remaining Contract period or the standard OEM warranty, whichever is longer.

### **7.16 Exit Management and Handover**

Upon expiry or termination of the Contract, the bidder shall provide all necessary assistance for smooth transition of the operations to the Tenderer or its nominated agency.

The bidder shall hand over all documents, configurations, licenses, reports, passwords (through a secure mechanism), backups, inventory details and any other information required for continued operation of the network without disruption.

## 7.17 Onsite Technical Support Manpower

1. The successful bidder shall deploy **minimum manpower as defined under RFP** at the Tenderer's premises throughout the Warranty and O&M period.
2. The deployed engineer shall be responsible for providing day-to-day operational support for the complete network infrastructure supplied under this Contract, including but not limited to:
  - A. Monitoring the health and availability of all active network devices.
  - B. First-level fault diagnosis and troubleshooting.
  - C. Incident logging, tracking and coordination for resolution.
  - D. Preventive maintenance activities.
  - E. Routine configuration support approved by the Tenderer.
  - F. Physical verification of network equipment.
  - G. Coordination with OEM Technical Assistance Centre (TAC).
  - H. Support during firmware upgrades, security patch deployment and planned maintenance activities.
  - I. Maintenance of asset inventory, incident records and documentation.
  - J. Submission of periodic reports as specified in the RFP.
  - K. Assisting the Tenderer during inspections, audits and acceptance activities.
3. The deployed engineer shall possess adequate technical qualifications and relevant experience in installation, configuration, operation and maintenance of enterprise network infrastructure, including switching, wireless networking, firewalls and network management systems. The engineer shall preferably possess valid OEM certifications relevant to the offered solution.
4. The deployed engineer shall report to the designated officer of the Tenderer and shall perform duties during normal office working hours. However, the bidder shall ensure availability of technical support beyond office hours, including weekends, public holidays and emergencies, whenever required for restoration of services within the prescribed SLA timelines.
5. The deployment of onsite engineer shall be considered the **minimum support requirement**. The bidder shall deploy **additional technical manpower, field engineers, cabling technicians, wireless engineers, security specialists or any other skilled resources, as may be required**, at its own cost, to meet the implementation schedule, warranty obligations and Service Level Agreements (SLAs). No additional payment shall be made by the Tenderer for deployment of such additional resources.
6. The bidder shall ensure that absence, leave, resignation or replacement of the deployed onsite engineer does not affect service delivery. A suitable replacement of equivalent or higher qualifications and experience shall be deployed immediately to ensure uninterrupted support.
7. During major incidents, preventive maintenance activities, firmware upgrades, network expansion, security incidents, FAT, audits or any activity requiring additional

- technical expertise, the bidder shall deploy adequate manpower, including OEM-certified engineers, without any additional financial implication to the Tenderer.
8. The bidder shall remain solely responsible for achieving all SLA requirements, irrespective of the number of personnel deployed. Deployment of onsite manpower shall not limit the bidder's responsibility to provide additional resources whenever necessary for timely restoration of services and successful operation of the network.
  9. The bidder shall ensure continuous coordination between the onsite engineer, bidder's backend support team and the respective OEM support team to facilitate timely incident resolution and effective network operations.
  10. The resident manpower shall mark attendance in the manner prescribed by the Tenderer and maintain daily activity logs. Quarterly attendance records, preventive maintenance reports, incident reports, and work completion reports shall be submitted along with the quarterly invoice.
  11. The bidder shall replace any resident manpower found unsuitable or whose performance is unsatisfactory as per instruction by the Tenderer, without any additional cost.
  12. In the event of resignation, transfer, long leave, illness, termination, or non-availability of any deployed manpower, the Bidder shall deploy a replacement resource of the same or higher qualification, experience, and skill level immediately without impact of services.
  13. Any period during which the minimum prescribed manpower is not available at site, or where the replacement resource does not meet the minimum qualification and experience requirements specified in the RFP, shall be treated as manpower non-availability for the purpose of SLA compliance. The Tenderer shall be entitled to apply pro-rata deductions/service credits for the actual period of such non-compliance, without prejudice to any other contractual remedies.
  14. Following are minimum qualification requirement of resources to be deploy

| Resource           | Qualification                           | Experience      |
|--------------------|-----------------------------------------|-----------------|
| Network Engineer   | BE/B.Tech(IT/EC/CS) + OEM Certification | Minimum 5 years |
| Network Technician | Diploma/ITI                             | Minimum 3 years |

## 7.18. Comprehensive Warranty

1. The bidder shall provide comprehensive Warranty and O&M Support Services for the complete solution for a period of Five (5) years. In addition, the bidder shall obtain and submit an OEM-backed Twenty-Five (25) Year System Performance and Application Assurance Warranty for the complete Structured Cabling System as specified in this RFP.
2. The warranty shall be **comprehensive**, covering all hardware, software, firmware, licenses, subscriptions, accessories, structured cabling, passive infrastructure, installation workmanship and all other components supplied and installed under this Contract, without any additional cost to the Tenderer.
3. During the Warranty period, the bidder shall provide comprehensive Operations & Maintenance (O&M) services, including but not limited to:

- a. Corrective Maintenance.
  - b. Preventive Maintenance.
  - c. Fault diagnosis and troubleshooting.
  - d. Replacement of defective equipment.
  - e. Software updates and firmware upgrades.
  - f. Security patches and bug fixes.
  - g. Configuration management.
  - h. Performance monitoring and optimization.
  - i. Incident management.
  - j. Technical support.
  - k. Submission of periodic reports.
  - l. OEM Technical Assistance Centre (TAC) support.
4. The bidder shall replace any defective or failed hardware, accessories or passive components with new or OEM-certified equivalent components of equal or higher specifications, without any additional financial implication to the Tenderer.
  5. The warranty shall cover replacement of all supplied equipment due to manufacturing defects, hardware failures, and failures arising during normal operating conditions, including failures caused by voltage fluctuations. The bidder shall provide and install all recommended power protection devices, surge protection, grounding, and earthing arrangements necessary for safe operation of the equipment. Damage caused by force majeure events, lightning strikes, fire, flood, theft, vandalism, deliberate misuse, or sustained electrical conditions beyond the OEM-specified operating limits shall be excluded unless otherwise covered by the bidder.
  6. All replacements shall be carried out in accordance with the Service Level Agreements (SLAs) specified in this RFP. Temporary workarounds shall not be treated as permanent resolution.
  7. The bidder shall ensure uninterrupted validity of all OEM warranties, software subscriptions, software licenses and support services throughout the Warranty period.
  8. Preventive Maintenance shall be carried out at least once every six (6) months or at such higher frequency as recommended by the OEM, with submission of detailed Preventive Maintenance Reports to the Tenderer.
  9. The bidder shall deploy and maintain the minimum onsite technical manpower specified in this RFP and shall arrange additional technical resources, including OEM specialists, whenever required to meet the prescribed SLA timelines and operational requirements. Deployment of additional manpower shall be entirely at the bidder's cost.
  10. Any equipment replaced during the Warranty period shall continue to be covered under warranty for the remaining Contract period or the standard OEM warranty applicable to the replacement equipment, whichever is longer.
  11. The bidder shall ensure availability of all necessary spare parts, consumables, software, firmware, tools, test equipment and technical resources required for maintenance of the complete solution throughout the Warranty period.
  12. Failure to meet the prescribed Service Levels during the Warranty period shall attract penalties as specified in the SLA section of this RFP.

13. Expiry of the Warranty period shall not relieve the bidder of its responsibility to rectify defects, deficiencies or latent faults identified prior to expiry of the Warranty period until such defects have been fully resolved to the satisfaction of the Tenderer.

---

## ***SECTION 8***

### ***Contract Period /Cancellation / Termination***

---

#### **8.1. Contract Period**

- a. The Contract shall become effective from the date of issuance of the Letter of Acceptance (LoA) / Work Order by the Tenderer and shall remain valid until successful completion of all contractual obligations, including implementation, Final Acceptance Testing (FAT), Go-Live, Warranty Support Services, submission of all deliverables, and settlement of all contractual obligations, unless terminated earlier in accordance with the provisions of the Contract.
- b. The successful bidder shall complete the supply, installation, integration, testing, commissioning, FAT and Go-Live of the complete Wi-Fi Infrastructure within the timelines specified in the RFP.
- c. Following successful Go-Live and issuance of the Final Acceptance Certificate (FAC), the bidder shall provide comprehensive Warranty and Operations & Maintenance (O&M) Support Services for a period of Five (5) years.
- d. The Contract shall remain in force during the entire Warranty and O&M period, including any approved extension, until all contractual obligations of both parties have been fulfilled.
- e. The Tenderer reserves the right to extend the Contract, if considered necessary in the interest of the project, on the same terms and conditions or on mutually agreed terms, subject to satisfactory performance of the bidder and applicable Government policies.

## 8.2. Termination for Default

The Tenderer may terminate the Contract, in whole or in part, by giving **thirty (30) days' written notice** to the successful bidder, if the bidder:

- a. Fails to supply, install, configure, integrate, test, commission or successfully complete the project within the timelines specified in the Contract.
- b. Fails to achieve Final Acceptance Testing (FAT), Go-Live or Final Acceptance Certificate (FAC) within the stipulated period.
- c. Fails to comply with the Service Level Agreements (SLAs) or repeatedly fails to restore services within the prescribed response and resolution timelines.
- d. Fails to rectify defects, deficiencies or observations pointed out by the Tenderer within the specified time.
- e. Abandons the project or suspends work without prior written approval of the Tenderer.
- f. Fails to deploy the required technical manpower or maintain the support services specified in the Contract.
- g. Fails to maintain valid OEM support, software subscriptions, licenses or warranty obligations during the Contract period.
- h. Commits a material breach of any provision of the Contract and fails to remedy such breach within the period specified by the Tenderer.

### **8.3. Termination for Insolvency**

The Tenderer may terminate the Contract with immediate effect if the bidder:

- a. Becomes insolvent or bankrupt.
- b. Enters into liquidation, winding-up or receivership proceedings.
- c. Makes any arrangement with creditors that materially affects its ability to perform the Contract.
- d. Ceases to carry on its business.

### **8.4 Termination for Non-Performance**

The Tenderer may terminate the Contract if:

- a. The bidder fails to successfully complete FAT after **two (2) attempts**.
- b. The bidder fails to meet mandatory technical, functional, interoperability, security or performance requirements specified in the RFP.
- c. Critical observations raised during FAT or Go-Live remain unresolved beyond the period specified by the Tenderer.

### **8.5. Termination for Regulatory or Security Non-Compliance**

The Tenderer may terminate the Contract if the bidder:

- a. Fails to comply with applicable laws, Government of India or Government of Gujarat guidelines.
- b. Fails to comply with directions issued by CERT-In, MeitY, DoT, TRAI or any other competent statutory authority applicable to the project.
- c. Introduces any security vulnerability or unauthorized software that materially compromises the security of the network.

### **8.6. Termination for Fraud, Corrupt or Unethical Practices**

The Tenderer may terminate the Contract with immediate effect if the bidder:

- a. Engages in fraudulent, corrupt, collusive or coercive practices.
- b. Submits forged, false or misleading documents or information.
- c. Obtains the Contract through misrepresentation.

## **8.7. Termination for Convenience**

The Tenderer reserves the right to terminate the Contract, in whole or in part, at any time in the public interest or due to administrative, financial or policy reasons by giving **thirty (30) days' written notice** to the bidder.

In such event, the bidder shall be entitled only to payment for the work satisfactorily completed and accepted by the Tenderer up to the effective date of termination. The bidder shall not be entitled to claim any compensation for anticipated profits, consequential losses or damages arising out of such termination.

## **8.8. Partial Termination**

The Tenderer may terminate the Contract in respect of specific sites, locations, buildings, components or services without affecting the remaining scope of the Contract.

The bidder shall continue to perform the remaining obligations under the Contract.

## **8.9. Consequences of Termination**

Upon termination, the bidder shall immediately:

- a. Stop all further work as directed by the Tenderer.
- b. Protect all completed work and equipment.
- c. Hand over all supplied equipment, configurations, licenses, documentation, reports, drawings, source files, backups, passwords (through a secure mechanism), asset registers and any other project-related records.
- d. Cooperate with the Tenderer for orderly transition of the services.

## **8.10. Risk and Cost Purchase**

If the Contract is terminated due to default of the bidder, the Tenderer shall have the right to complete the remaining work through any alternate agency.

Any additional expenditure incurred by the Tenderer for completion of the balance work shall be recoverable from the bidder, including adjustment against pending payments, Performance Bank Guarantee (PBG) or any other amount payable under the Contract.

## **8.11. Recovery of Dues**

The Tenderer shall have the right to recover any outstanding dues, penalties, damages, excess payments, risk purchase costs or any other recoverable amount from:

- a. Pending payments.

- b. Quarterly Warranty Payments.
- c. Performance Bank Guarantee.
- d. Any other amount payable to the bidder under this Contract.

#### **8.12. Blacklisting / Debarment**

Without prejudice to any other contractual rights, the Tenderer may recommend blacklisting/debarment of the bidder in accordance with the applicable Government rules and procedures in cases involving:

- a. Fraudulent or corrupt practices.
- b. Submission of false information or forged documents.
- c. Wilful breach of contractual obligations.
- d. Persistent or repeated non-performance.
- e. Abandonment of the project.

#### **8.13. Survival of Obligations**

Termination or expiry of the Contract shall not affect the rights and obligations of either party accrued prior to the date of termination, including obligations relating to confidentiality, intellectual property, warranties, indemnity, recovery of dues, dispute resolution and audit.

#### **8.14. General Contract Provisions**

##### **Governing Law and Jurisdiction**

The Contract shall be governed by the laws of India. Subject to the arbitration provision, courts at Gandhinagar, Gujarat, shall have exclusive jurisdiction.

##### **Dispute Resolution and Arbitration**

Any dispute shall first be referred to the authorized representatives of both parties for amicable resolution within thirty (30) days. If unresolved, the dispute shall be referred to a mutually appointed sole arbitrator in accordance with the Arbitration and Conciliation Act, 1996, as amended. The seat and venue of arbitration shall be Gandhinagar, Gujarat, and proceedings shall be conducted in English.

##### **Confidentiality and Data Ownership**

The Bidder shall maintain confidentiality of all information, data, configurations, credentials and records accessed under the Contract. All Tenderer data, logs, configurations, reports and

project-specific documents shall remain the exclusive property of the Tenderer and shall be handed over upon request, expiry or termination of the Contract.

#### Intellectual Property Rights

Pre-existing intellectual property of either party or OEM shall remain with its respective owner. The Tenderer shall have a perpetual, non-exclusive and royalty-free right to use all software licences, configurations, documentation and project-specific deliverables supplied under the Contract for its internal operations.

#### Indemnity and Liability

The Bidder shall indemnify the Tenderer against claims, losses, damages, penalties and expenses arising from breach of Contract, negligence, statutory non-compliance, bodily injury, property damage, data breach or intellectual-property infringement attributable to the Bidder. The Bidder's aggregate liability shall be limited to the Total Contract Value, except in cases of fraud, wilful misconduct, confidentiality/data breach, intellectual-property infringement, bodily injury, death or statutory liability.

#### Insurance

The Bidder shall maintain adequate employee compensation, personal accident, third-party liability, transit, installation and other applicable insurance throughout the Contract period and submit evidence whenever required.

#### Audit

The Tenderer or its authorized agency may inspect and audit project records, licences, invoices, SLA reports, configurations, security controls and contractual compliance. The Bidder shall provide necessary records and assistance without additional cost.

#### Assignment and Subcontracting

The Bidder shall not assign or subcontract any material contractual obligation without prior written approval of the Tenderer. Such approval shall not relieve the Bidder of any responsibility or liability under the Contract.

#### Change Control

Any change in scope, quantity, specification, timeline or price shall be implemented only through a written change order approved by the Tenderer. No verbal instruction shall entitle the Bidder to additional payment or extension of time.

#### Force Majeure

Neither party shall be liable for delay caused by events beyond its reasonable control, provided the affected party notifies the other party within seven (7) days, submits supporting evidence and takes reasonable measures to mitigate the impact. The affected timelines may

be extended proportionately. If the event continues beyond ninety (90) days, either party may seek termination of the affected scope without liability for future performance.

#### Termination for Convenience

The Tenderer may terminate the Contract, wholly or partly, for convenience by giving thirty (30) days' written notice. The Bidder shall be paid for satisfactorily completed and accepted work, conforming material delivered or irrevocably committed for the project, and approved non-cancellable OEM orders supported by documentary evidence. The Bidder shall take reasonable steps to cancel or minimize outstanding commitments. Upon payment, ownership of the corresponding material, licences and deliverables shall vest with the Tenderer. No payment shall be admissible for anticipated profit or consequential loss on the terminated scope.

#### Risk Purchase

Where the Bidder fails to perform its contractual obligations, the Tenderer shall issue written notice specifying the default and allow fifteen (15) days for rectification, except in an emergency requiring immediate action. If the default continues, the Tenderer may procure the outstanding goods or services from an alternate source at the risk and cost of the Bidder. The reasonable excess cost over the corresponding contracted value, after adjustment of the unexecuted scope, shall be recoverable from pending payments, the PBG or any other amount payable to the Bidder. The Bidder shall be informed of the recoverable amount with supporting details and shall remain responsible for obligations already performed or accepted.

---

***SECTION 9***

***Price BID***

---

**PRICE BID FORMAT:**

| Sr. No | Item Category                                       | Total Amount (Incl. GST) |
|--------|-----------------------------------------------------|--------------------------|
| A      | Total of Active-SITC                                |                          |
| B      | Total of Passive-SITC                               |                          |
| C      | Total of Resident Operations & Maintenance Manpower |                          |
| D      | Buyback of Existing IT & Wi-Fi Infrastructure       |                          |
| E      | <b>Grand Total (A+B+C-D)</b>                        |                          |

**BOQ LINE ITEM:**

| Sr. No | Category    | Item Description                                                                                                                                                                                                                                    | Approved /Eligible OEMs                    | Offered Make & Model | Unit | Qty | Unit Rate (Incl. GST) | Total Amount (Incl. GST) |
|--------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|----------------------|------|-----|-----------------------|--------------------------|
| A1     | Active-SITC | Next-Generation Firewall Appliance with redundant power supplies, rack-mount kit, required interfaces and optics, all specified security subscriptions/software licences for five years and five-year OEM support.                                  | <b>Cisco, Palo Alto Networks, Fortinet</b> |                      | Nos  | 2   |                       |                          |
| A2     | Active-SITC | Layer-3 Core Switch complete with Software Licenses, Redundant Power Supplies, Redundant Fan Trays, Rack Mounting Kit, Accessories, OEM Warranty & Support and all required transceivers/interconnect cables/AOC as per Technical Specifications.   |                                            |                      | Nos  | 2   |                       |                          |
| A3     | Active-SITC | Layer-3 Distribution Switch complete with Software Licenses, Uplink Module(s), Redundant Power Supplies, Redundant Fan Trays, Rack Mounting Kit, Accessories, OEM Warranty & Support and all required transceivers as per Technical Specifications. |                                            |                      | Nos  | 8   |                       |                          |
| A4     | Active-SITC | 24-Port Managed Gigabit Ethernet Access Switch complete with Software Licenses, Uplink Module(s), Rack Mounting Kit, Power Cord, Accessories and OEM Warranty & Support and all required transceivers as per Technical Specifications.              |                                            |                      | Nos  | 35  |                       |                          |
| A5     | Active-SITC | 48-Port Managed Gigabit Ethernet Access Switch complete with Software Licenses, Uplink Module(s), Rack Mounting Kit, Power Cord, Accessories                                                                                                        |                                            |                      | Nos  | 14  |                       |                          |

|     |             |                                                                                                                                                                                                                                                                                                      |     |     |  |  |  |  |
|-----|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|-----|--|--|--|--|
|     |             | and OEM Warranty & Support and all required transceivers as per Technical Specifications.                                                                                                                                                                                                            |     |     |  |  |  |  |
| A6  | Active-SITC | Wireless LAN Controller complete with all hardware, software licenses, access point capacity licenses, redundant PSU (where applicable), accessories, Warranty, OEM Support and all required transceivers as per Technical Specifications.                                                           | Nos | 2   |  |  |  |  |
| A7  | Active-SITC | Type-A : High-Performance Indoor Wi-Fi 7 Access Point complete with Ceiling/Wall Mounting Kit, Power Accessories (where applicable), Software Licenses (if applicable), OEM Warranty & Support for 5 year as per Technical Specifications..                                                          | Nos | 189 |  |  |  |  |
| A8  | Active-SITC | Type-B : Standard Indoor Wi-Fi 7 Access Point complete with Ceiling/Wall Mounting Kit, Power Accessories (where applicable), Software Licenses (if applicable), OEM Warranty & Support for 5 year as per Technical Specifications.                                                                   | Nos | 50  |  |  |  |  |
| A9  | Active-SITC | Type-C: Ruggedized Outdoor Wi-Fi 6E Access Point with IP66/IP67 or better enclosure, weatherproof mounting kit, required antennas, surge/power accessories where applicable, wireless-management licences/subscriptions for five years and five-year OEM support.                                    | Nos | 33  |  |  |  |  |
| A10 | Active-SITC | Type-D: High-Density Indoor/Outdoor Wi-Fi 7 Access Point complete with approved mounting kit, required antennas, power accessories where applicable, wireless-management licences/subscriptions for five years and five-year OEM support.                                                            | Nos | 168 |  |  |  |  |
| A11 | Active-SITC | Complete Centralized Network Management System (NMS) Solution complete with Hardware Appliance or Virtual Appliance (as applicable), Database, Operating System (if required), Software Licenses, Accessories, OEM Warranty & Support and all required transceivers as per Technical Specifications. | Nos | 1   |  |  |  |  |

|          |                             |                                                                                                                                                                                                                                                                                                     |                                |  |     |      |  |  |
|----------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|--|-----|------|--|--|
| A12      | Active-SITC                 | Network Access Control (NAC) Solution with Hardware Appliance or Virtual Appliance (as applicable), Software Licenses, Endpoint Licenses/subscription, Database, Operating System (if required), Accessories, OEM Warranty & Support and all required transceivers as per Technical Specifications. |                                |  | Nos | 2    |  |  |
| <b>A</b> | <b>Total of Active-SITC</b> |                                                                                                                                                                                                                                                                                                     |                                |  |     |      |  |  |
| B1       | Passive-SITC                | 06 Core Single Mode Armoured OS2 Optical Fiber Cable                                                                                                                                                                                                                                                | <b>CommScope/Molex/Legrand</b> |  | Mtr | 2700 |  |  |
| B2       | Passive-SITC                | 12 Core Single Mode Armoured OS2 Optical Fiber Cable                                                                                                                                                                                                                                                |                                |  | Mtr | 6600 |  |  |
| B3       | Passive-SITC                | 24 Core Single Mode Armoured OS2 Optical Fiber Cable                                                                                                                                                                                                                                                |                                |  | Mtr | 4200 |  |  |
| B4       | Passive-SITC                | 48 Core Single Mode Armoured OS2 Optical Fiber Cable                                                                                                                                                                                                                                                |                                |  | Mtr | 700  |  |  |
| B5       | Passive-SITC                | 12 Port Rack Mount LIU Fully Loaded (LC Duplex SM)                                                                                                                                                                                                                                                  |                                |  | Nos | 10   |  |  |
| B6       | Passive-SITC                | 24 Port Rack Mount LIU Fully Loaded (LC Duplex SM)                                                                                                                                                                                                                                                  |                                |  | Nos | 54   |  |  |
| B7       | Passive-SITC                | 48 Port Rack Mount LIU Fully Loaded (LC Duplex SM)                                                                                                                                                                                                                                                  |                                |  | Nos | 13   |  |  |
| B8       | Passive-SITC                | 96 Port Rack Mount LIU Fully Loaded (LC Duplex SM)                                                                                                                                                                                                                                                  |                                |  | Nos | 3    |  |  |
| B9       | Passive-SITC                | LC-LC Single Mode Duplex Patch Cord 3 Mtr                                                                                                                                                                                                                                                           |                                |  | Nos | 220  |  |  |
| B10      | Passive-SITC                | LC-LC Single Mode Duplex Patch Cord 10 Mtr                                                                                                                                                                                                                                                          |                                |  | Nos | 3    |  |  |
| B11      | Passive-SITC                | Cat6A Structured Cabling Data Point (Complete SITC)                                                                                                                                                                                                                                                 |                                |  | Nos | 235  |  |  |
| B12      | Passive-SITC                | Cat6A Structured Cabling Wi-Fi Access Point Outlet (Complete SITC)                                                                                                                                                                                                                                  |                                |  | Nos | 450  |  |  |
| B13      | Passive-SITC                | Cat6A Indoor UTP Cable (305 Mtr Box)                                                                                                                                                                                                                                                                |                                |  | Box | 175  |  |  |
| B14      | Passive-SITC                | Cat6A Outdoor UTP Cable (305 Mtr Box)                                                                                                                                                                                                                                                               |                                |  | Box | 30   |  |  |
| B15      | Passive-SITC                | Cat6A Keystone Jack                                                                                                                                                                                                                                                                                 |                                |  | Nos | 306  |  |  |
| B16      | Passive-SITC                | Single Port Face Plate                                                                                                                                                                                                                                                                              |                                |  | Nos | 306  |  |  |
| B17      | Passive-SITC                | Cat6A 24 Port Loaded Patch Panel                                                                                                                                                                                                                                                                    |                                |  | Nos | 56   |  |  |
| B18      | Passive-SITC                | Cat6A Patch Cord 1 Mtr                                                                                                                                                                                                                                                                              |                                |  | Nos | 794  |  |  |
| B19      | Passive-SITC                | Cat6A Patch Cord 2 Mtr                                                                                                                                                                                                                                                                              |                                |  | Nos | 600  |  |  |

|     |              |                                                                                                                            |
|-----|--------------|----------------------------------------------------------------------------------------------------------------------------|
| B20 | Passive-SITC | Cat6A RJ45 Connector                                                                                                       |
| B21 | Passive-SITC | Shielded Metal RJ45 Connector for Outdoor Wi-Fi                                                                            |
| B22 | Passive-SITC | 42U Rack Complete with PDU, Fan Tray, Cable Manager, Shelves (where applicable), Earthing Kit and Accessories.             |
| B23 | Passive-SITC | 24U Floor Mount Rack Complete with PDU, Fan Tray, Cable Manager, Shelves (where applicable), Earthing Kit and Accessories. |
| B24 | Passive-SITC | 12U Floor Mount Rack Complete with PDU, Fan Tray, Cable Manager, Shelves (where applicable), Earthing Kit and Accessories. |
| B25 | Passive-SITC | 9U Wall Mount Rack Complete with PDU, Fan Tray, Cable Manager, Shelves (where applicable), Earthing Kit and Accessories.   |
| B26 | Passive-SITC | 6U IP65 Outdoor Rack                                                                                                       |
| B27 | Passive-SITC | 25 mm HDPE Pipe                                                                                                            |
| B28 | Passive-SITC | PVC Back Box                                                                                                               |
| B29 | Passive-SITC | 32 mm Reinforced Flexible Pipe                                                                                             |
| B30 | Passive-SITC | 25 mm PVC Conduit with Accessories                                                                                         |
| B31 | Passive-SITC | 32 mm PVC Flexible Pipe                                                                                                    |
| B32 | Passive-SITC | MS Clamp for AP Mounting                                                                                                   |
| B33 | Passive-SITC | 3 Mtr Standard GI Pole                                                                                                     |
| B34 | Passive-SITC | Laying of 6/12 Core Armoured Optical Fiber Cable                                                                           |
| B35 | Passive-SITC | Laying of 24/48 Core Armoured Optical Fiber Cable                                                                          |
| B36 | Passive-SITC | Laying of 25 mm HDPE Pipe & 32 mm Reinforced Flexible Pipe                                                                 |
| B37 | Passive-SITC | Installation/Fixing of LIU                                                                                                 |
| B38 | Passive-SITC | Fiber Pigtail Splicing (Per Core)                                                                                          |
| B39 | Passive-SITC | Fiber Testing (OTDR / OLTS / Power Meter)                                                                                  |
| B40 | Passive-SITC | Laying of Cat6A UTP Cable                                                                                                  |

|  |     |       |  |  |
|--|-----|-------|--|--|
|  | Nos | 600   |  |  |
|  | Nos | 100   |  |  |
|  | Nos | 1     |  |  |
|  | Nos | 3     |  |  |
|  | Nos | 1     |  |  |
|  | Nos | 11    |  |  |
|  | Nos | 10    |  |  |
|  | Mtr | 11000 |  |  |
|  | Nos | 350   |  |  |
|  | Mtr | 1000  |  |  |
|  | Mtr | 17833 |  |  |
|  | Mtr | 900   |  |  |
|  | Nos | 100   |  |  |
|  | Nos | 25    |  |  |
|  | Mtr | 9200  |  |  |
|  | Mtr | 4800  |  |  |
|  | Mtr | 12000 |  |  |
|  | Nos | 80    |  |  |
|  | Nos | 1572  |  |  |
|  | Nos | 1572  |  |  |
|  | Mtr | 68000 |  |  |

|          |                                            |                                                                                                     |           |  |          |       |  |  |
|----------|--------------------------------------------|-----------------------------------------------------------------------------------------------------|-----------|--|----------|-------|--|--|
| B41      | Passive-SITC                               | Installation of PVC Conduit/Flexible Pipe with Accessories                                          |           |  | Mtr      | 17000 |  |  |
| B42      | Passive-SITC                               | Ferruling & Labelling of UTP Cable                                                                  |           |  | Nos      | 576   |  |  |
| B43      | Passive-SITC                               | Installation of Face Plate with Back Box                                                            |           |  | Nos      | 350   |  |  |
| B44      | Passive-SITC                               | Termination of Information Outlet                                                                   |           |  | Nos      | 350   |  |  |
| B45      | Passive-SITC                               | Installation, Dressing and Termination of 24-Port Cat6A Loaded Patch Panel                          |           |  | Nos      | 55    |  |  |
| B46      | Passive-SITC                               | Installation of 3 Mtr Pole with Foundation                                                          |           |  | Nos      | 25    |  |  |
| B47      | Passive-SITC                               | Installation of MS Clamp for AP Mounting                                                            |           |  | Nos      | 100   |  |  |
| B48      | Passive-SITC                               | Soft Soil Excavation, Backfilling and Route Restoration                                             |           |  | Mtr      | 3450  |  |  |
| B49      | Passive-SITC                               | RCC / CC / Asphalt Road Cutting and Restoration                                                     |           |  | Mtr      | 300   |  |  |
| B50      | Passive-SITC                               | Installation of 42U Rack with Cable Dressing                                                        |           |  | Nos      | 1     |  |  |
| B51      | Passive-SITC                               | Installation of 24U Rack with Cable Dressing                                                        |           |  | Nos      | 3     |  |  |
| B52      | Passive-SITC                               | Installation of 12U Rack with Cable Dressing                                                        |           |  | Nos      | 1     |  |  |
| B53      | Passive-SITC                               | Installation of 9U Wall Mount Rack with Cable Dressing                                              |           |  | Nos      | 11    |  |  |
| B54      | Passive-SITC                               | Installation of 6U Outdoor IP65 Rack with Cable Dressing                                            |           |  | Nos      | 10    |  |  |
| B55      | Passive-SITC                               | UTP Cable Testing                                                                                   |           |  | Nos      | 650   |  |  |
| <b>B</b> | <b>Total of Passive-SITC</b>               |                                                                                                     |           |  |          |       |  |  |
| C1       | Resident Operations & Maintenance Manpower | Network Engineer (Active Component) for Operation & Maintenance during Warranty Period (5 Years)    | <b>NA</b> |  | Resource | 1     |  |  |
| C2       | Resident Operations & Maintenance Manpower | Network Technician (Passive Component) for Operation & Maintenance during Warranty Period (5 Years) | <b>NA</b> |  | Resource | 1     |  |  |

|          |                                                                |                                                          |           |  |                 |  |  |  |
|----------|----------------------------------------------------------------|----------------------------------------------------------|-----------|--|-----------------|--|--|--|
| <b>C</b> | <b>Total of Resident Operations &amp; Maintenance Manpower</b> |                                                          | <b>NA</b> |  |                 |  |  |  |
| <b>D</b> | <b>Buyback</b>                                                 | <b>Buyback of Existing IT &amp; Wi-Fi Infrastructure</b> | <b>NA</b> |  | <b>Lump sum</b> |  |  |  |
| <b>E</b> | <b>Grand Total (A+B+C-D)</b>                                   |                                                          |           |  |                 |  |  |  |

## General BOQ Conditions

1. The quoted rates shall be inclusive of supply, installation, testing, commissioning, integration, configuration, freight, transit insurance, loading/unloading, documentation, OEM support, warranty, taxes and duties, labour, consumables, tools & tackles, accessories, and all incidental expenses necessary for successful completion of the work, unless specifically stated otherwise in the RFP.
2. The offered equipment shall be supplied complete with all required OEM-certified/OEM-supported optical transceivers, AOC/DAC cables, stacking/virtual-switching cables, breakout/adaptor modules, patch cords and other interconnect accessories necessary to implement the approved network architecture and port-to-port connectivity. The bidder shall include the complete quantity and cost of such components in the respective equipment line item, and no separate payment shall be admissible. The bidder shall submit a component-wise OEM Bill of Material, including part numbers, quantities, interface type, media, wavelength and supported reach.
3. The BOQ shall be read in conjunction with the Technical Specifications, Scope of Work, and all other provisions of the RFP. Any hardware, software, licenses, accessories, consumables, mounting hardware, connectors, adapters, patch cords, transceivers, cables, tools, services, or any other items required for successful installation, integration, testing, commissioning, operation, and acceptance of the complete solution, but not specifically listed in the BOQ, shall be deemed to be included in the quoted prices. No additional payment shall be admissible on this account.
4. The bidder shall quote for all BOQ line items. Partial quoting, omission of any mandatory BOQ item, or quoting multiple makes/models or optional products against a single BOQ line item shall render the bid liable for rejection. The bidder shall quote only one Make and Model against each BOQ line item.

5. The offered make and model for each BOQ item shall strictly comply with the Technical Specifications prescribed in the RFP. Any deviation shall be evaluated in accordance with the provisions of the RFP.
6. The quantities indicated in the BOQ are tentative and are provided only for the purpose of bid evaluation. The Tenderer reserves the right to increase, decrease, omit, or add quantities during execution based on the actual site requirements. Payment shall be made only for the actual quantities supplied, installed, tested, commissioned, and accepted by the Tenderer or its authorized agency, unless otherwise specified in the RFP.
7. All active components shall be supplied complete with the required software licenses, subscriptions, and accessories, mounting hardware, rack mounting kits, power cords, transceivers, cables, documentation, OEM support, and all associated components necessary for successful operation of the offered solution, unless separately identified in the BOQ.
8. All passive components shall be supplied complete with compatible accessories, consumables, fixing materials, connectors, mounting hardware, and other associated items necessary for successful installation, testing, commissioning, and operation, unless separately identified in the BOQ.
9. Any infrastructure upgrades, additional accessories, software licenses, transceivers, power supplies, structured cabling modifications, server/storage infrastructure for log retention, or any other hardware or software required to implement and operate the proposed solution in compliance with the Technical Specifications, DoT, CERT-In, and other applicable statutory guidelines shall be deemed to be included in the quoted prices. No separate payment shall be admissible on this account.
10. The successful bidder shall deploy the minimum resident Operation & Maintenance manpower specified in the BOQ throughout the Warranty/O&M period. In addition, the bidder shall deploy adequate qualified technical manpower, either onsite or offsite, as and when required for preventive maintenance, corrective maintenance, fault rectification, upgrades, project implementation, FAT, Go-Live activities, or to meet the prescribed SLA requirements, without any additional financial implication to the Tenderer.
11. Wherever the BOQ specifies a complete system or equipment, the quoted price shall be deemed to include all associated hardware, software, operating system (where applicable), database (where applicable), licenses, subscriptions, optics, DAC/AOC cables, mounting hardware, accessories, documentation, OEM warranty, OEM support, and all other components necessary for successful installation, commissioning, integration, and operation of the offered solution, whether or not individually listed in the BOQ.
12. Any infrastructure upgrade required for successful deployment and operation of the proposed Wi-Fi 7 solution shall be included in the bidder's quoted prices. No additional payment shall be made on this account.
13. Additional Manpower may be deployed on Pro-rata basis and on demand basis as per the requirement of the Office as when required for the event.
14. The bidder shall quote the **buyback value** for the existing infrastructure separately in the prescribed BOQ inclusive of applicable taxes. The quoted buyback value shall be deducted from the total project cost for the purpose of financial evaluation and payment, as specified in the BOQ.

15. Financial ranking, including determination of the L1 bidder, shall be based on the Evaluated Grand Total (E), inclusive of GST.

---

***SECTION 10***  
***SPECIFICATION***

---

## 10.1 Active Component:

| Item Code : A-1                                              |                      |                                                                                                                                                                                                                                                                                   |                     |
|--------------------------------------------------------------|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| Name of Item : Next-Generation Firewall (NGFW)               |                      |                                                                                                                                                                                                                                                                                   |                     |
| Approved/Eligible OEMs : Cisco, Palo Alto Networks, Fortinet |                      |                                                                                                                                                                                                                                                                                   |                     |
| Sr. No.                                                      | Section              | Technical Specification                                                                                                                                                                                                                                                           | Compliance (Yes/No) |
| 1                                                            | General / Functional | The proposed security platform shall provide stateful firewalling, application visibility and control, and intrusion prevention functionality from Day 1.                                                                                                                         |                     |
| 2                                                            | General / Functional | The appliance should support at least 8 x RJ45 1G, 8 x 1/10/25G and 4 * 40G SFP+ interfaces from day 1.                                                                                                                                                                           |                     |
| 3                                                            | General / Functional | The proposed appliance shall be sized and configured to meet all specified performance, session, logging, HA and security requirements. The OEM shall declare the offered CPU architecture, system memory and usable local storage in its bid.                                    |                     |
| 4                                                            | General / Functional | The proposed firewall may use general-purpose processors, security processors, ASICs or an equivalent architecture, provided all quoted performance is achieved with the required security services enabled.                                                                      |                     |
| 5                                                            | General / Functional | Performance figures shall be supported by an OEM datasheet or an independently verifiable test report and shall apply to the offered hardware/software configuration with the specified security functions enabled.                                                               |                     |
| 6                                                            | General / Functional | Proposed Firewall shall be rack mountable in standard rack.                                                                                                                                                                                                                       |                     |
| 7                                                            | General / Functional | The firewall shall deliver at least 20 Gbps threat-protection/NGFW throughput with firewalling, application visibility and control, and IPS enabled, based on an OEM-published enterprise traffic profile or independently verifiable test methodology.                           |                     |
| 8                                                            | General / Functional | Firewall should support atleast 4 Million concurrent sessions with application visibility turned on                                                                                                                                                                               |                     |
| 9                                                            | General / Functional | The firewall shall support at least 150,000 new connections per second with application visibility enabled, at least 19 Gbps IPsec VPN throughput, and at least 6,000 site-to-site/remote-access VPN peers in the offered configuration.                                          |                     |
| 10                                                           | General / Functional | Firewall should have integrated redundant hot-swappable power supply and redundant hot-swappable fan-tray/modules from Day 1. All the Power supplies and Fantray/module shall be hot-swappable and no downtime/ reboot shall be required addtiona/removal of fantray/fans/module. |                     |

|    |                      |                                                                                                                                                                                                                                                                                                                                                                 |  |
|----|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 11 | General / Functional | High Availability Configurations shall support Active/Passive or Active/Active- Clustering                                                                                                                                                                                                                                                                      |  |
| 12 | General / Functional | The firewall shall provide a unified access-control policy framework supporting rules based on IPv4/IPv6 objects, users and user groups, applications, URL categories, geolocation, security zones, VLANs, interfaces, services and ports. Multiple criteria shall be combinable in a single rule.                                                              |  |
| 13 | General / Functional | Firewall should support static NAT, dynamic NAT, dynamic pat                                                                                                                                                                                                                                                                                                    |  |
| 14 | General / Functional | Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to- IPv6) functionality                                                                                                                                                                                                                                                       |  |
| 15 | General / Functional | Should support Static, RIP, OSPF, OSPFv3 and BGP, BGPv6                                                                                                                                                                                                                                                                                                         |  |
| 16 | General / Functional | The proposed firewall shall support at least 10 independent virtual firewall instances (such as virtual systems, contexts, VDOMs or equivalent), with separate routing and security policies and traffic/configuration isolation. Configurable resource allocation or limits shall be supported. All required licences shall be included from Day 1.            |  |
| 17 | General / Functional | Should support Multicast protocols like IGMP, PIM, etc                                                                                                                                                                                                                                                                                                          |  |
| 18 | General / Functional | Should support capability to create multiple virtual context/instance with strict hardware resource (CPU, Memory & Storage) reservation and ensure traffic isolation between virtual context/instance                                                                                                                                                           |  |
| 19 | General / Functional | Should support capability to integrate with other security solutions to receive contextual information like security group tags/names                                                                                                                                                                                                                           |  |
| 20 | General / Functional | Should have the capability of passively gathering information about virtual machine traffic, network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance. |  |
| 21 | General / Functional | Should support more than 4000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness and should be able to create 40 or more application categories for operational efficiency                                                                                          |  |
| 22 | General / Functional | Should be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.                                                                                                                                                                                                 |  |
| 23 | General / Functional | Should support more than 25,000 (excluding custom signatures) IPS signatures or more. Should support capability to configure correlation rule where multiple rules/event can be combined together for better efficacy                                                                                                                                           |  |

|    |                      |                                                                                                                                                                                                                                        |  |
|----|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 24 | General / Functional | Should be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports.                                                                                      |  |
| 25 | General / Functional | Should be able to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events.                                                                                                                    |  |
| 26 | General / Functional | Should be capable of detecting and blocking IPv6 attacks.                                                                                                                                                                              |  |
| 27 | General / Functional | The solution should be able to identify, decrypt and evaluate both inbound and outbound SSL traffic on-box                                                                                                                             |  |
| 28 | General / Functional | Should support the capability to quarantine end point by integrating with other security solution like Network Admission Control                                                                                                       |  |
| 29 | General / Functional | The solution must provide IP reputation feed that comprised of several regularly updated collections of poor reputation of IP addresses determined by the proposed security vendor                                                     |  |
| 30 | General / Functional | Solution must support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist                                                                                                  |  |
| 31 | General / Functional | Should must support DNS threat intelligence feeds to protect against threats                                                                                                                                                           |  |
| 32 | General / Functional | The Appliance OEM must have its own threat intelligence analysis center and should use the global footprint of security deployments for more comprehensive network protection.                                                         |  |
| 33 | General / Functional | The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).                                         |  |
| 34 | General / Functional | Should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location                                                                                                                       |  |
| 35 | General / Functional | The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioural anomaly detection techniques. |  |
| 36 | General / Functional | Should support Open based Application ID / Custom Application ID for access to community resources and ability to easily customize security to address new and specific threats and applications quickly                               |  |
| 37 | General / Functional | Should support URL threat intelligence feeds to protect against threats                                                                                                                                                                |  |
| 38 | General / Functional | Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies on a continuously updated URL reputation and category database.                 |  |

|                        |                         |                                                                                                                                                                                                                                                                                                                          |  |
|------------------------|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 39                     | General /<br>Functional | Should support safe-search and restricted-content enforcement for supported search engines and online video platforms                                                                                                                                                                                                    |  |
| 40                     | General /<br>Functional | The management platform must be accessible via a web-based interface and ideally with no need for additional client software.                                                                                                                                                                                            |  |
| 41                     | General /<br>Functional | The management platform must domain multi-domain management.                                                                                                                                                                                                                                                             |  |
| 42                     | General /<br>Functional | The management platform must be a dedicated OEM appliance or VM based solution.                                                                                                                                                                                                                                          |  |
| 43                     | General /<br>Functional | The management platform must provide centralized logging and reporting functionality                                                                                                                                                                                                                                     |  |
| 44                     | General /<br>Functional | The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows                                                                                                                                                       |  |
| 45                     | General /<br>Functional | The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.                                                                                                                   |  |
| 46                     | General /<br>Functional | Should support packet-path analysis, policy simulation and packet-capture troubleshooting capabilities                                                                                                                                                                                                                   |  |
| 47                     | General /<br>Functional | Should support REST API for monitoring and config programmability                                                                                                                                                                                                                                                        |  |
| 48                     | General /<br>Functional | The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.                                                                                                                                                                                                                |  |
| 49                     | General /<br>Functional | The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).                                                                                                                                                                                                                |  |
| 50                     | General /<br>Functional | The centralized management platform must not have any limit in terms of handling logs per day                                                                                                                                                                                                                            |  |
| 51                     | General /<br>Functional | Solution should be able to provide insights of hosts/user on basis of indication of compromise, any license required for this to be included from day one                                                                                                                                                                |  |
| 52                     | General /<br>Functional | The management platform must provide built-in robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.                                                                                                                      |  |
| 53                     | General /<br>Functional | The management platform support running on-demand and scheduled reports                                                                                                                                                                                                                                                  |  |
| 54                     | General /<br>Functional | The management platform must risk reports like advanced malware, attacks and network                                                                                                                                                                                                                                     |  |
| 55                     | General /<br>Functional | The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools. |  |
| <b>Item Code : A-2</b> |                         |                                                                                                                                                                                                                                                                                                                          |  |

| Name of Item: Layer-3 Core Switch                 |                    |                                                                                                                                                                                                                                                                                                                                        |                     |
|---------------------------------------------------|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| Approved/Eligible OEMs : Cisco, HPE Aruba, Ruckus |                    |                                                                                                                                                                                                                                                                                                                                        |                     |
| Sr. No.                                           | Section            | Technical Specification                                                                                                                                                                                                                                                                                                                | Compliance (Yes/No) |
| 1                                                 | General Features   | Switch shall be rack mountable in standard rack.                                                                                                                                                                                                                                                                                       |                     |
| 2                                                 | General Features   | The solution should allow for network system virtualization technology that pairs two switches into one from perspective of neighboring switch. This helps in simplifying L2 and L3 topology and representing the virtualized system represent as a single spanning tree node for rest of the network and a single node for Management |                     |
| 3                                                 | General Features   | Switch should support features that can minimize the traffic downtime during software upgrade including ISSU, Non-stop routing/Non-stop Forwarding, Graceful Restart for routing protocols, Stateful Switchover and upgrading individual task/process without impacting hardware forwarding                                            |                     |
| 4                                                 | General Features   | Switch shall have hot swappable 1:1 redundant internal power supply and redundant fans.                                                                                                                                                                                                                                                |                     |
| 5                                                 | Performance        | Switch shall have minimum 16 GB RAM and minimum 16 GB Flash                                                                                                                                                                                                                                                                            |                     |
| 6                                                 | Performance        | The switch shall have minimum 6 Tbps of switching fabric and                                                                                                                                                                                                                                                                           |                     |
| 7                                                 | Performance        | Forwarding rates: The switch should have minimum 2000 Mpps of forwarding rate.                                                                                                                                                                                                                                                         |                     |
| 8                                                 | Performance        | IPv4 Routing entry support : 200K or more                                                                                                                                                                                                                                                                                              |                     |
| 9                                                 | Performance        | IPv6 Routing entry support : 200K or more                                                                                                                                                                                                                                                                                              |                     |
| 10                                                | Performance        | Multicast Routing entry support : 30 K or more                                                                                                                                                                                                                                                                                         |                     |
| 11                                                | Performance        | MAC addresses support: 64 K or more                                                                                                                                                                                                                                                                                                    |                     |
| 12                                                | Performance        | VLANs 1K                                                                                                                                                                                                                                                                                                                               |                     |
| 13                                                | Performance        | ACL & QOS entry support : 16K or more                                                                                                                                                                                                                                                                                                  |                     |
| 14                                                | Performance        | Packet buffer : 30 MB or more                                                                                                                                                                                                                                                                                                          |                     |
| 15                                                | Performance        | IPv6 support in hardware, providing wire rate forwarding for IPv6 network                                                                                                                                                                                                                                                              |                     |
| 16                                                | L2 and L3 Features | Switch should support IPFRR for OSPF which helps to restores the layer 3 traffic during both link and node failures in the layer 3 network.                                                                                                                                                                                            |                     |
| 17                                                | L2 and L3 Features | Should support IEEE Standards of Ethernet: IEEE 802.1D, 802.1s, 802.1w, 802.1x, 802.3ad, 802.3x, 802.1p, 802.1Q, 1588v2/NTP, 802.1AE, IEEE 802.1ab, 802.1BA, PVLAN, UDLD, IGMP and QinQ.                                                                                                                                               |                     |
| 18                                                | L2 and L3 Features | Must support RIP, BGP, IS-IS, BSR, MSDP, PIM SM, PIM SSM, PIM-BIDIR, IP SLA, OSPF, VRF, VXLAN, BGP-EVPN, MPLS, mVPN,                                                                                                                                                                                                                   |                     |
| 19                                                | L2 and L3 Features | Administrator should be able to influence the loadsharing over Portchannel using multiple inputs like combination of source and destination Mac Address, VLAN, L3 IP and L4 port numbers                                                                                                                                               |                     |

|    |                    |                                                                                                                                                                                                                                                    |  |
|----|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 20 | L2 and L3 Features | Switch should be able to be configured with per port MTU                                                                                                                                                                                           |  |
| 21 | L2 and L3 Features | Switch should allow user to configure a pair of a Layer 2 interfaces (trunk ports or port channels) where one interface is configured to act as a backup to the other, thus providing an alternative solution to the Spanning Tree Protocol (STP). |  |
| 22 | L2 and L3 Features | Switch should support VRRPv2 (RFC3768) and VRRPv3 (RFC 5798),                                                                                                                                                                                      |  |
| 23 | L2 and L3 Features | Should support mechanism to suppress the effects of excessive interface flapping events on routing protocols and routing tables in the network                                                                                                     |  |
| 24 | Security           | Switch should allow to display an error message and shut down the port when a loop is detected                                                                                                                                                     |  |
| 25 | Security           | Switch should be able to support IP ACLs, port ACLs, VLAN ACLs, MAC ACLs and IPV6 ACLs. Administrator should have option to define time of day and the week for the ACLs to be active.                                                             |  |
| 26 | Security           | Switch should support 802.1X, MAB and Web-based authentication                                                                                                                                                                                     |  |
| 27 | Security           | Switch should support IP Source Guard and Unicast RPF check to protect the network against spoofed source IP traffic                                                                                                                               |  |
| 28 | Security           | Switch shall support Unknown Unicast Flood Blocking, Broadcast storm control and Multicast storm control in hardware on all ports.                                                                                                                 |  |
| 29 | Security           | Shall support DHCP Snooping, Dynamic ARP Inspection, Control Plane Policing, Port Security,                                                                                                                                                        |  |
| 30 | Security           | Switch should support Dynamic VLAN assignment, wake-on-LAN (WOL) technology,                                                                                                                                                                       |  |
| 31 | Security           | Switch must support a means of separately authenticating users when multiple hosts are connected to a single port.                                                                                                                                 |  |
| 32 | Security           | Switch should support IPv6 security including IPv6 FHS Binding Table, IPv6 ND Inspection, IPv6 RA Guard, IPv6 DHCP Guard and IPv6 Source Guard,                                                                                                    |  |
| 33 | Security           | Switch should support Layer-2 256-bit AES-GCM symmetric encryption between switches over 1/10/25G and 40/100G (at line-rate)                                                                                                                       |  |
| 34 | Security           | Switch should support RadSec over TLS and DTLS                                                                                                                                                                                                     |  |
| 35 | Security           | Switch should have online diagnostics capabilities during bootup to check different hardware components and verify the data path and the control signals. Similar capability should be available either via on-demand or can be scheduled          |  |
| 36 | QoS                | Eight egress queues per port for different types.                                                                                                                                                                                                  |  |
| 37 | QoS                | Switch should trust Trust/untrust all incoming packets based on DSCP/IPPreC/COS/Exp marking by default.                                                                                                                                            |  |
| 38 | QoS                | Switch should support various ingress QoS mechanisms including Traffic classification utilizing                                                                                                                                                    |  |

|    |                                    |                                                                                                                                                                                                                                                                 |  |
|----|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
|    |                                    | ACL,DSCP,CoS,EXP,VLAN and IPP, Conditional remarking and policing                                                                                                                                                                                               |  |
| 39 | QoS                                | Switch should support various egress QoS mechanisms including Traffic classification, Egress Marking, CBWFQ Egress Queuing, policing and shaping                                                                                                                |  |
| 40 | QoS                                | Switch should support application of queuing policies on individual sub-interfaces                                                                                                                                                                              |  |
| 41 | QoS                                | Switch should be able to support Multiple Strict Priority Queuing (min 2) and other queues should support Weighted Round Robin (WRR)/Weighted Fair Queueing (WFQ)/Weighted Tail Drop (WTD)                                                                      |  |
| 42 | QoS                                | Switch should support active queue management like WTD and WRED should be available                                                                                                                                                                             |  |
| 43 | QoS                                | Switch shall support Single Rate Two Color and Two Rate Three Color policer                                                                                                                                                                                     |  |
| 44 | QoS                                | The switches must support marking/remarking based on the following mappings from DSCP to 802.1p and 802.1p to DSCP.                                                                                                                                             |  |
| 45 | QoS                                | Switch shall support application visibility and traffic monitoring with minimum 1K or more sflow/jflow/netFlow/Clearflow entries.                                                                                                                               |  |
| 46 | Management and Monitoring Features | Switch should support simplified VLAN management across multiple switches in a network and shall support authentication for the same.                                                                                                                           |  |
| 47 | Management and Monitoring Features | Switch should be able to share vlan information about all the vlans including PVLAN and MST Vlan information.                                                                                                                                                   |  |
| 48 | Management and Monitoring Features | Switch should support Telnet, SSH, SFTP and SCP file transfer,                                                                                                                                                                                                  |  |
| 49 | Management and Monitoring Features | Switch should support Configuration Change Notification and Logging, including the ability to track the name of the user that executed a command                                                                                                                |  |
| 50 | Management and Monitoring Features | Switch offers the ability to monitor events and take informational, corrective, or any desired action when the monitored events occur or when a threshold is reached.                                                                                           |  |
| 51 | Management and Monitoring Features | Proposed switch should support NTPv4, RMON (RFC 1757, 2896, 3919, 4502) and IPFIX/sFlow/NetFlow or equivalent or equivalent/equivalent.                                                                                                                         |  |
| 52 | Management and Monitoring Features | Proposed switch should support SNMPv1 (RFC 1157), SNMPv2c (RFC 3416, 3417) and SNMPv3 (RFC 3548, 3826)                                                                                                                                                          |  |
| 53 | Management and Monitoring Features | Platform should support device login authentication and authorization via RADIUS/TACACS+/Local login. Switch should have ability to designate one or more protocols to be used for AAA, thus ensuring a backup system for AAA in case the initial method fails. |  |
| 54 | Management and Monitoring Features | Switch should have capability to check the status of copper cabling, L2 Traceroute,                                                                                                                                                                             |  |

|    |                                    |                                                                                                                                                                                                                                                                                                                                                                      |  |
|----|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 55 | Management and Monitoring Features | Switch should be able to generate traffic in a continuous, reliable, and predictable manner, for measuring network performance. It should collect and provide data about response time, one- way latency, jitter (interpacket delay variance), packet loss, voice quality scoring, network resource availability, application performance, and server response time. |  |
| 56 | Programmability                    | During system boots, the system's software signatures should be checked for integrity. System should capable to understand that system OS are authentic and unmodified, it should have cryptographically signed images to provide assurance that the firmware & BIOS are authentic.                                                                                  |  |
| 57 | Programmability                    | Switch should support NETCONF/YANG, RESTCONF, MDT and gNMI programmatic interface,                                                                                                                                                                                                                                                                                   |  |
| 58 | Programmability                    | Switch should support Day 0 provisioning automation with Secure ZTP (RFC8572).                                                                                                                                                                                                                                                                                       |  |
| 59 | Programmability                    | Switch should support automated network boot/provisioning through iPXE or an equivalent mechanism over IPv4 and IPv6, where required                                                                                                                                                                                                                                 |  |
| 60 | Programmability                    | Switch should support on-box scripting or equivalent API-driven automation                                                                                                                                                                                                                                                                                           |  |
| 61 | Programmability                    | Shall support Single Operating System binary image for all switch models proposed as part of the design.                                                                                                                                                                                                                                                             |  |
| 62 | Interface                          | Switch should have minimum Interface - 32 x 40/100G ports                                                                                                                                                                                                                                                                                                            |  |
| 63 | Interface                          | Switch should have a RJ45/USB Based Console Port                                                                                                                                                                                                                                                                                                                     |  |
| 64 | Interface                          | Should have Ethernet RJ-45 OOB Management Port.                                                                                                                                                                                                                                                                                                                      |  |
| 65 | Certification                      | Switch should support secure data wipe as per NIST 3 standard                                                                                                                                                                                                                                                                                                        |  |
| 66 | Certification                      | Switch shall conform to EN 60950-1, IEC 62368-1, CISPR 32, EN 300 386, EN61000-3-2, EN 55032 and 47 CFR Part 15 Class A Standards                                                                                                                                                                                                                                    |  |
| 67 | Certification                      | The device should be IPv6 ready and NDcPP / EAL Certified under Common Criteria from day one                                                                                                                                                                                                                                                                         |  |

**Item Code : A-3**

**Name of Item : Layer-3 Distribution Switch**

**Approved/Eligible OEMs : Cisco, HPE Aruba, Ruckus**

| Sr. No. | Section                  | Technical Specification                                                                                                                                                                                    | Compliance (Yes/No) |
|---------|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| 1       | Hardware and Performance | Switch should be fixed configuration 1 RU platform to support atleast 12* 1/10/25 Gigabit ports and 2 nos. of 40G/100G Uplink ports. And should be populated with transceivers as per the Interface table. |                     |
| 2       | Hardware and Performance | Switch should support Internal redundant power supplies                                                                                                                                                    |                     |
| 3       | Hardware and Performance | Should have 16 GB RAM and 16 GB Flash                                                                                                                                                                      |                     |

|    |                          |                                                                                                                                                                                                                                                                                                                                   |  |
|----|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 4  | Hardware and Performance | Switch should have non blocking architecture and should support switching capacity of 1000 Gbps                                                                                                                                                                                                                                   |  |
| 5  | Hardware and Performance | Switch should support at least 744.04 Mpps throughput from day-1                                                                                                                                                                                                                                                                  |  |
| 6  | Hardware and Performance | The switches shall support physical stacking or an equivalent virtual switching/cluster technology that provides a single logical control/management plane and resilient forwarding. The proposed design shall include all required interfaces, licences and cables and shall meet the required aggregate inter-switch bandwidth. |  |
| 7  | L2 Feature               | Switch should support at least 32K Mac address                                                                                                                                                                                                                                                                                    |  |
| 8  | L2 Feature               | Switch should support Ethernet standards like IEEE802.1p, IEEE802.1Q, Jumbo frame, 802.1D, 802.1w, 802.1s, Jumbo frames, 802.3ad,                                                                                                                                                                                                 |  |
| 9  | L2 Feature               | Switch should support 4000 vlans and 1000 SVI                                                                                                                                                                                                                                                                                     |  |
| 10 | L2 Feature               | Switch should support vlans based on ports, MAC address, IP-Subnet based vlan                                                                                                                                                                                                                                                     |  |
| 11 | L2 Feature               | The switch shall support standards-based neighbour discovery through LLDP and LLDP-MED, together with an equivalent unidirectional-link-failure detection mechanism where required.                                                                                                                                               |  |
| 12 | L3 Features              | Switch should support 24K IPv4 and 19K IPv6 entries                                                                                                                                                                                                                                                                               |  |
| 13 | L3 Features              | Switch should support up to 8K multicast routes                                                                                                                                                                                                                                                                                   |  |
| 14 | L3 Features              | Switch should support routing protocols like BGPv4, OSPF(v2, v3), ISIS, RIP, Static,VXLAN, PIM, SSM, DVMRP, BFD                                                                                                                                                                                                                   |  |
| 15 | L3 Features              | The switch shall support VRRP or an equivalent standards-based first-hop redundancy mechanism.                                                                                                                                                                                                                                    |  |
| 16 | L3 Features              | Switch should support VRF, MPLS, Policy based routing                                                                                                                                                                                                                                                                             |  |
| 17 | L3 Features              | Switch should support RFC 7252 (CoAP)                                                                                                                                                                                                                                                                                             |  |
| 18 | QoS features             | Switch should support 8 queues per port                                                                                                                                                                                                                                                                                           |  |
| 19 | QoS features             | The switch should support Standard 802.1p CoS field classification                                                                                                                                                                                                                                                                |  |
| 20 | QoS features             | The switch should support IPSLA feature set to verify services guarantee based on business critical IP Applications.                                                                                                                                                                                                              |  |
| 21 | QoS features             | The switch should support QoS based on application                                                                                                                                                                                                                                                                                |  |
| 22 | Security                 | Switch should support at least 8K hardware based ACL                                                                                                                                                                                                                                                                              |  |
| 23 | Security                 | Switch should support IP Source guard and DHCP Snooping                                                                                                                                                                                                                                                                           |  |
| 24 | Security                 | Switch should support 802.1x for user authentication and authorization, Dynamic vlan assignment                                                                                                                                                                                                                                   |  |
| 25 | Security                 | The switch shall support hardware-assisted flow telemetry using IPFIX, sFlow, NetFlow or equivalent, sized for the project's monitoring requirement. The bidder shall state the supported active-flow scale.                                                                                                                      |  |
| 26 | Security                 | The switch should support MAC address notification to allow administrators to be notified of users added to or removed from the network.                                                                                                                                                                                          |  |

|    |                                |                                                                                                                                                                                                                                                                                      |  |
|----|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 27 | Security                       | Switch should have unique secure identity so that it's authenticity and origin can be confirmed with OEM. Switch BIOS, software image should be cryptographically signed to ensure integrity and switch should not boot with modified software regardless of user's privilege level. |  |
| 28 | Security                       | Switch should support IEEE 802.1AE AES 256 for link encryption from day 1                                                                                                                                                                                                            |  |
| 29 | Management and Troubleshooting | Switch should support telnet, ssh, https, SNMPv3, IPFIX/sFlow/NetFlow or equivalent feature for ease of management                                                                                                                                                                   |  |
| 30 | Management and Troubleshooting | Switch should support API Driven configuration and support Netconf and Restconf using YANG data model. It should support automation tool like python                                                                                                                                 |  |
| 31 | Management and Troubleshooting | Switch should support features like RSPAN, ERSPAN                                                                                                                                                                                                                                    |  |
| 32 | Management and Troubleshooting | Switch should able to support container to run applications. Switch should provide ability to automate the process of upgrading software images and installing configuration files on switches when they are being deployed in the network for the first time.                       |  |
| 33 | Management and Troubleshooting | The switch should support Layer 2 trace route to ease troubleshooting by identifying the physical path that a packet takes from source to destination.                                                                                                                               |  |
| 34 | Management and Troubleshooting | The switch should support asset identification and inventory management through a physical asset tag, electronic identifier, barcode/QR code or equivalent mechanism                                                                                                                 |  |
| 35 | Management and Troubleshooting | Switch should be populated with redundant AC power supplies                                                                                                                                                                                                                          |  |
| 36 | Management and Troubleshooting | Switches need to be provided with required software license from day-1 as per RFP specification                                                                                                                                                                                      |  |
| 37 | Certification                  | Switch shall conform to UL 60950, IEC 60950, EN 55032 Class A, CISPR 32 Class A Standards                                                                                                                                                                                            |  |
| 38 | Certification                  | Switch / Switch's Operating System should be tested for EAL 2/NDPP/NIAP or above under Common Criteria Certification.                                                                                                                                                                |  |

**Item Code : A-4**

**Name of Item : 24-Port Multigigabit PoE Access Switch**

**Approved/Eligible OEMs : Cisco, HPE Aruba, Ruckus**

| Sr. No. | Section                  | Technical Specification                                                                                                                                                                                                                                                                                                | Compliance (Yes/No) |
|---------|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| 1       | Hardware and Performance | The switch shall be a fixed-configuration, rack-mountable platform with at least 24 multigigabit access ports supporting 100M/1G/2.5G/5G/10G with IEEE 802.3bt Class 6 PoE (minimum 60W per supported port), and at least 2 x 25GbE uplinks. Higher-speed uplinks may be provided through fixed or modular interfaces. |                     |

|    |                          |                                                                                                                                                                                                                                                                                                                                   |  |
|----|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 2  | Hardware and Performance | Switch should support Internal redundant platinum rated power supplies                                                                                                                                                                                                                                                            |  |
| 3  | Hardware and Performance | Should have 16 GB RAM and 16 GB Flash                                                                                                                                                                                                                                                                                             |  |
| 4  | Hardware and Performance | Switch should have non blocking architecture and should support switching capacity of 580 Gbps                                                                                                                                                                                                                                    |  |
| 5  | Hardware and Performance | Switch should support at least 400 Mpps throughput from day-1                                                                                                                                                                                                                                                                     |  |
| 6  | Hardware and Performance | The switches shall support physical stacking or an equivalent virtual switching/cluster technology that provides a single logical control/management plane and resilient forwarding. The proposed design shall include all required interfaces, licences and cables and shall meet the required aggregate inter-switch bandwidth. |  |
| 7  | L2 Feature               | Switch should support at least 32K Mac address                                                                                                                                                                                                                                                                                    |  |
| 8  | L2 Feature               | Switch should support Ethernet standards like IEEE802.1p, IEEE802.1Q, 802.1D, 802.1w, 802.1s, 802.3ad.                                                                                                                                                                                                                            |  |
| 9  | L2 Feature               | Switch should support 4000 vlans and 1000 SVI                                                                                                                                                                                                                                                                                     |  |
| 10 | L2 Feature               | Switch should support vlans based on ports, MAC address, IP-Subnet based vlan                                                                                                                                                                                                                                                     |  |
| 11 | L2 Feature               | The switch shall support standards-based neighbour discovery through LLDP and LLDP-MED, together with an equivalent unidirectional-link-failure detection mechanism where required.                                                                                                                                               |  |
| 12 | L2 Feature               | The switch shall support jumbo Ethernet frames of at least 9,000 bytes.                                                                                                                                                                                                                                                           |  |
| 13 | L3 Features              | Switch should support 18K IPv4/IPv6 entries                                                                                                                                                                                                                                                                                       |  |
| 14 | L3 Features              | Switch should have capability to support up to 8K multicast routes                                                                                                                                                                                                                                                                |  |
| 15 | L3 Features              | Switch should support full L3 functionality if needed by upgrading the license later.                                                                                                                                                                                                                                             |  |
| 16 | L3 Features              | The switch shall support VRRP or an equivalent standards-based first-hop redundancy mechanism.                                                                                                                                                                                                                                    |  |
| 17 | L3 Features              | Switch should have the capability to support network segmentation that overcomes the limitation of VLANs using VXLAN and VRFs by upgrading the license as necessary                                                                                                                                                               |  |
| 18 | L3 Features              | Switch should have 16 MB or more packet buffer.                                                                                                                                                                                                                                                                                   |  |
| 19 | L3 Features              | QoS features                                                                                                                                                                                                                                                                                                                      |  |
| 20 | L3 Features              | The switch should support Standard 802.1p CoS field classification                                                                                                                                                                                                                                                                |  |
| 21 | L3 Features              | Switch shall have classification, marking, policing and shaping and eight egress queues.                                                                                                                                                                                                                                          |  |
| 22 | L3 Features              | The switch should support IPSLA or equivalent feature set to verify services guarantee based on business critical IP Applications.                                                                                                                                                                                                |  |
| 23 | L3 Features              | The switch should support QoS based on application                                                                                                                                                                                                                                                                                |  |
| 24 | L3 Features              | Security                                                                                                                                                                                                                                                                                                                          |  |
| 25 | L3 Features              | Switch should support at least 5K hardware based ACL                                                                                                                                                                                                                                                                              |  |

|                        |             |                                                                                                                                                                                                                                                                                      |  |
|------------------------|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 26                     | L3 Features | Switch should support IP Source guard and DHCP Snooping                                                                                                                                                                                                                              |  |
| 27                     | L3 Features | Switch should support 802.1x for user authentication and authorization, Dynamic vlan assignment                                                                                                                                                                                      |  |
| 28                     | L3 Features | The switch shall support hardware-assisted flow telemetry using IPFIX, sFlow, NetFlow or equivalent, sized for the project's monitoring requirement. The bidder shall state the supported active-flow scale.                                                                         |  |
| 29                     | L3 Features | The switch should support MAC address notification to allow administrators to be notified of users added to or removed from the network.                                                                                                                                             |  |
| 30                     | L3 Features | Switch should support IPv6 Binding Integrity Guard, IPv6 Snooping, IPv6 RA Guard, IPv6 DHCP Guard, IPv6 Neighbor Discovery Inspection and IPv6 Source Guard.                                                                                                                         |  |
| 31                     | L3 Features | Switch should have unique secure identity so that it's authenticity and origin can be confirmed with OEM. Switch BIOS, software image should be cryptographically signed to ensure integrity and switch should not boot with modified software regardless of user's privilege level. |  |
| 32                     | L3 Features | Switch should support IEEE 802.1AE for link encryption from day 1                                                                                                                                                                                                                    |  |
| 33                     | L3 Features | Management and Troubleshooting                                                                                                                                                                                                                                                       |  |
| 34                     | L3 Features | Switch should support telnet, ssh, https, SNMPv3, IPFIX/sFlow/NetFlow or equivalent feature for ease of management                                                                                                                                                                   |  |
| 35                     | L3 Features | Switch should have capability to support API Driven configuration and support Netconf and Restconf using YANG data model. It should have capability to support automation tool like python                                                                                           |  |
| 36                     | L3 Features | Switch should support Manual/CLI or WebUI configuration of SPAN, RSPAN for providing near real-time access to operational statistics.                                                                                                                                                |  |
| 37                     | L3 Features | The switch should support Layer 2 trace route to ease troubleshooting by identifying the physical path that a packet takes from source to destination.                                                                                                                               |  |
| 38                     | L3 Features | Switch should support real-time network event detection and onboard automation scripts                                                                                                                                                                                               |  |
| 39                     | L3 Features | Switch should be populated with redundant AC power supplies                                                                                                                                                                                                                          |  |
| 40                     | L3 Features | Switches need to be provided with required software license from day-1                                                                                                                                                                                                               |  |
| 41                     | L3 Features | Certification                                                                                                                                                                                                                                                                        |  |
| 42                     | L3 Features | Switch should be ROHS Certified                                                                                                                                                                                                                                                      |  |
| 43                     | L3 Features | Switch shall conform to UL 60950, IEC 60950, EN 55032 Class A, CISPR 32 Class A, CISPR 35 Standards                                                                                                                                                                                  |  |
| 44                     | L3 Features | Switch / Switch's Operating System should be tested for EAL 2/NDPP/NIAP or above under Common Criteria Certification.                                                                                                                                                                |  |
| <b>Item Code : A-5</b> |             |                                                                                                                                                                                                                                                                                      |  |

| Name of Item : 48-Port Multigigabit PoE Access Switch |                          |                                                                                                                                                                                                                                                                                                                                                                      |                     |
|-------------------------------------------------------|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| Approved/Eligible OEMs : Cisco, HPE Aruba, Ruckus     |                          |                                                                                                                                                                                                                                                                                                                                                                      |                     |
| Sr. No.                                               | Section                  | Technical Specification                                                                                                                                                                                                                                                                                                                                              | Compliance (Yes/No) |
| 1                                                     | Hardware and Performance | The switch shall be a fixed-configuration, rack-mountable platform with 48 multigigabit access ports, including at least 12 ports supporting 100M/1G/2.5G/5G/10G and remaining ports supporting at least 100M/1G/2.5G, with IEEE 802.3bt PoE as specified, and at least 2 x 25GbE uplinks. Higher-speed uplinks may be provided through fixed or modular interfaces. |                     |
| 2                                                     | Hardware and Performance | Switch should support Internal redundant platinum rated power supplies                                                                                                                                                                                                                                                                                               |                     |
| 3                                                     | Hardware and Performance | Should have 16 GB RAM and 16 GB Flash                                                                                                                                                                                                                                                                                                                                |                     |
| 4                                                     | Hardware and Performance | Switch should have non blocking architecture and should support switching capacity of 520 Gbps                                                                                                                                                                                                                                                                       |                     |
| 5                                                     | Hardware and Performance | Switch should support at least 400 Mpps throughput from day-1                                                                                                                                                                                                                                                                                                        |                     |
| 6                                                     | Hardware and Performance | The switches shall support physical stacking or an equivalent virtual switching/cluster technology that provides a single logical control/management plane and resilient forwarding. The proposed design shall include all required interfaces, licences and cables and shall meet the required aggregate inter-switch bandwidth.                                    |                     |
| 7                                                     | L2 Feature               | Switch should support at least 32K Mac address                                                                                                                                                                                                                                                                                                                       |                     |
| 8                                                     | L2 Feature               | Switch should support Ethernet standards like IEEE802.1p, IEEE802.1Q, 802.1D, 802.1w, 802.1s, 802.3ad.                                                                                                                                                                                                                                                               |                     |
| 9                                                     | L2 Feature               | Switch should support 4000 vlans and 1000 SVI                                                                                                                                                                                                                                                                                                                        |                     |
| 10                                                    | L2 Feature               | Switch should support vlans based on ports, MAC address, IP-Subnet based vlan                                                                                                                                                                                                                                                                                        |                     |
| 11                                                    | L2 Feature               | The switch shall support standards-based neighbour discovery through LLDP and LLDP-MED, together with an equivalent unidirectional-link-failure detection mechanism where required.                                                                                                                                                                                  |                     |
| 12                                                    | L2 Feature               | The switch shall support jumbo Ethernet frames of at least 9,000 bytes.                                                                                                                                                                                                                                                                                              |                     |
| 13                                                    | L3 Features              | Switch should support 18K IPv4/IPv6 entries                                                                                                                                                                                                                                                                                                                          |                     |
| 14                                                    | L3 Features              | Switch should have capability to support up to 8K multicast routes                                                                                                                                                                                                                                                                                                   |                     |
| 15                                                    | L3 Features              | The switch shall support VRRP or an equivalent standards-based first-hop redundancy mechanism.                                                                                                                                                                                                                                                                       |                     |
| 16                                                    | L3 Features              | Switch should support full L3 functionality if needed by upgrading the license later.                                                                                                                                                                                                                                                                                |                     |
| 17                                                    | L3 Features              | Switch should have the capability to support network segmentation that overcomes the limitation of VLANs                                                                                                                                                                                                                                                             |                     |

|    |             |                                                                                                                                                                                                                                                                                      |  |
|----|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
|    |             | using VXLAN and VRFs by upgrading the license as necessary                                                                                                                                                                                                                           |  |
| 18 | L3 Features | Switch should have 16 MB or more packet buffer.                                                                                                                                                                                                                                      |  |
| 19 | L3 Features | QoS features                                                                                                                                                                                                                                                                         |  |
| 20 | L3 Features | The switch should support Standard 802.1p CoS field classification                                                                                                                                                                                                                   |  |
| 21 | L3 Features | Switch shall have classification, marking, policing and shaping and eight egress queues.                                                                                                                                                                                             |  |
| 22 | L3 Features | The switch should support IPSLA or equivalent feature set to verify services guarantee based on business critical IP Applications.                                                                                                                                                   |  |
| 23 | L3 Features | The switch should support QoS based on application                                                                                                                                                                                                                                   |  |
| 24 | L3 Features | Security                                                                                                                                                                                                                                                                             |  |
| 25 | L3 Features | Switch should support at least 5K hardware based ACL                                                                                                                                                                                                                                 |  |
| 26 | L3 Features | Switch should support IP Source guard and DHCP Snooping                                                                                                                                                                                                                              |  |
| 27 | L3 Features | Switch should support 802.1x for user authentication and authorization, Dynamic vlan assignment                                                                                                                                                                                      |  |
| 28 | L3 Features | The switch shall support hardware-assisted flow telemetry using IPFIX, sFlow, NetFlow or equivalent, sized for the project's monitoring requirement. The bidder shall state the supported active-flow scale.                                                                         |  |
| 29 | L3 Features | The switch should support MAC address notification to allow administrators to be notified of users added to or removed from the network.                                                                                                                                             |  |
| 30 | L3 Features | Switch should support IPv6 Binding Integrity Guard, IPv6 Snooping, IPv6 RA Guard, IPv6 DHCP Guard, IPv6 Neighbor Discovery Inspection and IPv6 Source Guard.                                                                                                                         |  |
| 31 | L3 Features | Switch should have unique secure identity so that it's authenticity and origin can be confirmed with OEM. Switch BIOS, software image should be cryptographically signed to ensure integrity and switch should not boot with modified software regardless of user's privilege level. |  |
| 32 | L3 Features | Switch should support IEEE 802.1AE for link encryption from day 1                                                                                                                                                                                                                    |  |
| 33 | L3 Features | Management and Troubleshooting                                                                                                                                                                                                                                                       |  |
| 34 | L3 Features | Switch should support telnet, ssh, https, SNMPv3, IPFIX/sFlow/NetFlow or equivalent feature for ease of management                                                                                                                                                                   |  |
| 35 | L3 Features | Switch should support API Driven configuration and support Netconf and Restconf using YANG data model. It should support automation tool like python                                                                                                                                 |  |
| 36 | L3 Features | Switch should support Manual/CLI or WebUI configuration of SPAN, RSPAN for providing near real-time access to operational statistics.                                                                                                                                                |  |
| 37 | L3 Features | The switch should support Layer 2 trace route to ease troubleshooting by identifying the physical path that a packet takes from source to destination.                                                                                                                               |  |

| 38                                                               | L3 Features          | Switch should support real-time network event detection and onboard automation scripts                                                                                                                                                                                                         |                            |
|------------------------------------------------------------------|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| 39                                                               | L3 Features          | Switch should be populated with redundant AC power supplies                                                                                                                                                                                                                                    |                            |
| 40                                                               | L3 Features          | Switches need to be provided with required software license from day-1                                                                                                                                                                                                                         |                            |
| 41                                                               | L3 Features          | Certification                                                                                                                                                                                                                                                                                  |                            |
| 42                                                               | L3 Features          | Switch should be ROHS Certified                                                                                                                                                                                                                                                                |                            |
| 43                                                               | L3 Features          | Switch shall conform to UL 60950, IEC 60950, EN 55032 Class A, CISPR 32 Class A, CISPR 35 Standards                                                                                                                                                                                            |                            |
| 44                                                               | L3 Features          | Switch / Switch's Operating System should be tested for EAL 2/NDPP/NIAP or above under Common Criteria Certification.                                                                                                                                                                          |                            |
| <b>Item Code : A-6</b>                                           |                      |                                                                                                                                                                                                                                                                                                |                            |
| <b>Name of Item : Wireless LAN Controller / Gateway Solution</b> |                      |                                                                                                                                                                                                                                                                                                |                            |
| <b>Approved/Eligible OEMs : Cisco, HPE Aruba, Ruckus</b>         |                      |                                                                                                                                                                                                                                                                                                |                            |
| <b>Sr. No.</b>                                                   | <b>Section</b>       | <b>Technical Specification</b>                                                                                                                                                                                                                                                                 | <b>Compliance (Yes/No)</b> |
| 1                                                                | General / Functional | The proposed controller/gateway solution shall manage the complete offered AP fleet from Day 1 with at least 25% growth headroom and shall support at least 3,000 APs and 30,000 concurrent clients from day 1                                                                                 |                            |
| 2                                                                | General / Functional | The controller shall support deployment flexibility without compromising any features                                                                                                                                                                                                          |                            |
| 3                                                                | General / Functional | The offered controller/gateway architecture shall provide at least 50 Gbps aggregate encrypted WLAN data-plane capacity, or demonstrate that local/distributed forwarding removes the centralized tunnelling bottleneck while meeting the same client and application performance requirement. |                            |
| 4                                                                | General / Functional | The solution shall provide sufficient redundant 10/25/40/100GbE connectivity to meet the specified aggregate throughput and HA design. Exact interface type and count may vary by architecture and shall be detailed in the bid.                                                               |                            |
| 5                                                                | General / Functional | Wireless Controller shall support link aggregation and load sharing between Access Point to WLC links                                                                                                                                                                                          |                            |
| 6                                                                | General / Functional | The controller shall support hardware encrypted data plane between Access Point and Controller                                                                                                                                                                                                 |                            |
| 7                                                                | General / Functional | High Availability mode shall support controller inline data plane mode as well as local switching mode and Mesh mode                                                                                                                                                                           |                            |
| 8                                                                | General / Functional | High Availability mode shall allow geographically dispersed installation between Controllers                                                                                                                                                                                                   |                            |
| 9                                                                | General / Functional | The controller failover shall not trigger client de-authentication and re-association                                                                                                                                                                                                          |                            |
| 10                                                               | General / Functional | The redundant Controller shall sync Access Point and Client Status, including DHCP IP lease status                                                                                                                                                                                             |                            |

|    |                         |                                                                                                                                                                                                                                                                                                      |  |
|----|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 11 | General /<br>Functional | Access Point shall be able to proactively distributes Client connection before and after association and tracking client condition in real time using data packet RSSI                                                                                                                               |  |
| 12 | General /<br>Functional | The controller/gateway solution shall use a secure, authenticated and encrypted AP-to-controller/gateway control and data protocol, based on CAPWAP or an OEM-equivalent protocol. The bidder shall describe encryption, authentication, replay protection and vulnerability-remediation mechanisms. |  |
| 13 | General /<br>Functional | The controller shall support Inter-Controller Wireless Roaming                                                                                                                                                                                                                                       |  |
| 14 | General /<br>Functional | The controller shall maintains per-user Application usage and shall be able to export it for network analytic.                                                                                                                                                                                       |  |
| 15 | General /<br>Functional | The controller shall support Multi Languages options from embedded GUI Management                                                                                                                                                                                                                    |  |
| 16 | General /<br>Functional | The controller shall provide per-Client Connection Scoring and provide reasoning of Client Connection Score                                                                                                                                                                                          |  |
| 17 | General /<br>Functional | The controller shall support Cellular offload using IPv6 tunneling to Mobile Core network                                                                                                                                                                                                            |  |
| 18 | General /<br>Functional | The controller shall be able to support multiple RF Management profile per group of APs, including Transmit Power Control and Dynamic Channel Assignment on both 2.4GHz and 5Ghz                                                                                                                     |  |
| 19 | General /<br>Functional | The controller shall be able to identify and avoid interferers with network performance impact analysis report                                                                                                                                                                                       |  |
| 20 | General /<br>Functional | The controller shall support optimized, automatic channel width (20~160Mhz) selection over 5GHz, 802.11ac                                                                                                                                                                                            |  |
| 21 | General /<br>Functional | Mesh AP nodes shall provide quick convergence and fast failover to new root mesh node                                                                                                                                                                                                                |  |
| 22 | General /<br>Functional | Mesh Backhaul interface shall support full duplex operation using wired daisy chaining                                                                                                                                                                                                               |  |
| 23 | General /<br>Functional | Mesh AP shall support fast roaming for Wired-client through wired-to-wireless bridge client                                                                                                                                                                                                          |  |
| 24 | General /<br>Functional | The controller shall support per-user and per-WLAN based application recognition and control that throttle usage by rate-limiting                                                                                                                                                                    |  |
| 25 | General /<br>Functional | The controller application recognition technology shall support exporting to 3rd party compatible format, such as IPFIX, NetFlow, sFlow or an equivalent open/exportable flow format                                                                                                                 |  |
| 26 | General /<br>Functional | The controller shall provide policy-based mDNS gateway including chromecast gateway                                                                                                                                                                                                                  |  |
| 27 | General /<br>Functional | The contorller shall support new application signatures without upgrading controller software                                                                                                                                                                                                        |  |
| 28 | General /<br>Functional | The controller shall provide Device Profiling using mutlple profiling methods to reduce false-detection                                                                                                                                                                                              |  |

|    |                      |                                                                                                                                                                                             |  |
|----|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 29 | General / Functional | The system shall provide secure onboarding service for both employee and guest based on standard-based security protocol Proposed system shall not use public cloud as user data repository |  |
| 30 | General / Functional | The controller shall be able to embedded custom web portal page (HTML) to fully customize user experience without additional cost or extra box                                              |  |
| 31 | General / Functional | The controller shall provide rule-based rogue classification and automatically run rogue mitigation action                                                                                  |  |
| 32 | General / Functional | The controller shall support Content Security using DNS integration, Web Classification shall be fully customizable                                                                         |  |
| 33 | General / Functional | The system shall support control plane encryption on both IPv4 and IPv6                                                                                                                     |  |
| 34 | General / Functional | The Controller's image upgrade shall be done through secure, encrypted transport                                                                                                            |  |
| 35 | General / Functional | The controller shall be able to provide unique pre-shared keys to the devices that do not support the 802.1x security protocol                                                              |  |
| 36 | General / Functional | The controller shall support Identity PSK for on boarding                                                                                                                                   |  |
| 37 | General / Functional | The controller shall support identification & mitigation of threats inside encrypted traffic                                                                                                |  |
| 38 | General / Functional | WIPS should detect and protect an Ad-hoc connection when a connected user forming a network with other system without an AP or try enabling bridging between two interface                  |  |
| 39 | General / Functional | WIPS should detect if a user try to impersonate a management frame.                                                                                                                         |  |
| 40 | General / Functional | WIPS should detect and take appropriate containment action if a smartphone user using tethering to connect other device.                                                                    |  |
| 41 | General / Functional | WIPS functionality should be available on both centralized and distributed traffic forwarding mode from AP.                                                                                 |  |
| 42 | General / Functional | The solution should be able to detect wireless Denial of Service (DoS) attacks such as Disassociation flood, Disassociation broadcast, RTS/CTS flood, EAPOL log off, Association flood etc. |  |
| 43 | General / Functional | The WLC shall support protection from dragonblood backward compatibility attack with WPA3 authentication.                                                                                   |  |
| 44 | General / Functional | The controller shall support mapping of specific VLANs to single SSID, depending on Access Point location and user                                                                          |  |
| 45 | General / Functional | The controller shall support automatic VLAN assignment per SSID to load-balance user connection. assigned VLAN pool shall be same as number of available VLAN in the system                 |  |

| 46                                                                 | General / Functional | The controller shall support embedded best practice configuration profile and setup                                                                                                                                                                         |                            |
|--------------------------------------------------------------------|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| 47                                                                 | General / Functional | The controller shall support packet fragmentation between Access Point and controller communication                                                                                                                                                         |                            |
| <b>Item Code : A-7</b>                                             |                      |                                                                                                                                                                                                                                                             |                            |
| <b>Name of Item : High-Performance Indoor Wi-Fi 7 Access Point</b> |                      |                                                                                                                                                                                                                                                             |                            |
| <b>Approved/Eligible OEMs : Cisco, HPE Aruba, Ruckus</b>           |                      |                                                                                                                                                                                                                                                             |                            |
| <b>Sr. No.</b>                                                     | <b>Section</b>       | <b>Technical Specification</b>                                                                                                                                                                                                                              | <b>Compliance (Yes/No)</b> |
| 1                                                                  | General / Functional | The AP shall be Wi-Fi 7 tri-band and support concurrent operation in 2.4 GHz, 5 GHz and 6 GHz, with 4x4 MIMO radio architecture. MU-MIMO and Multi-Link Operation shall be supported.                                                                       |                            |
| 2                                                                  | General / Functional | The AP shall include integrated BLE and/or IEEE 802.15.4 IoT radio capability for location, asset-tracking or sensor use cases. Integrated GNSS, UWB or equivalent location enhancement may be offered where available.                                     |                            |
| 3                                                                  | General / Functional | The AP shall operate on IEEE 802.3at or 802.3bt PoE. The bidder shall disclose any feature or radio restrictions at each supported PoE level; the offered PoE design shall enable the required production radio configuration without material restriction. |                            |
| 4                                                                  | General / Functional | The AP shall support flexible radio operation or an equivalent mechanism for dynamically optimizing 2.4 GHz/5 GHz spectrum use according to the RF design.                                                                                                  |                            |
| 5                                                                  | General / Functional | The wireless solution shall provide dedicated or time-sliced spectrum analysis, WIDS/WIPS and off-channel RF monitoring without materially affecting client service. The bidder shall describe the implementation.                                          |                            |
| 6                                                                  | General / Functional | Access Point should have 1x 100M/1000M/2.5G/5G/10G Multigigabit Ethernet (RJ-45)                                                                                                                                                                            |                            |
| 7                                                                  | General / Functional | Access Point should have USB port for future requirement.                                                                                                                                                                                                   |                            |
| 8                                                                  | General / Functional | Must have atleast 5 dBi Antenna gain on each radios                                                                                                                                                                                                         |                            |
| 9                                                                  | General / Functional | The AP shall provide an aggregate maximum PHY data rate appropriate for the offered radio configuration and not less than 10 Gbps. The bidder shall state the per-band and aggregate PHY rates.                                                             |                            |
| 10                                                                 | General / Functional | Must support minimum of 23dbm of transmit power in all 2.4Ghz, 5Ghz & 6ghz radios. And should follow the local regulatory Norms.                                                                                                                            |                            |
| 11                                                                 | General / Functional | Must support AP enforced load-balance between 2.4Ghz and 5Ghz band.                                                                                                                                                                                         |                            |
| 12                                                                 | General / Functional | Must incorporate radio resource management for power, channel and performance optimization                                                                                                                                                                  |                            |
| 13                                                                 | General / Functional | Must have -98 dB or better Receiver Sensitivity.                                                                                                                                                                                                            |                            |

|                                                            |                      |                                                                                                                                                                                                                        |  |
|------------------------------------------------------------|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 14                                                         | General / Functional | Must support Proactive Key Caching and/or other methods for Fast Secure Roaming.                                                                                                                                       |  |
| 15                                                         | General / Functional | Must support Management Frame Protection.                                                                                                                                                                              |  |
| 16                                                         | General / Functional | Should support locally-significant certificates on the APs using a Public Key Infrastructure (PKI).                                                                                                                    |  |
| 17                                                         | General / Functional | Access Points must support Hardware-based encrypted user data and management traffic between controller and Access point for better security.                                                                          |  |
| 18                                                         | General / Functional | Must support the ability to serve clients and monitor the RF environment concurrently.                                                                                                                                 |  |
| 19                                                         | General / Functional | Same model AP that serves clients must be able to be dedicated to monitoring the RF environment.                                                                                                                       |  |
| 20                                                         | General / Functional | Must be plenum-rated (UL2043).                                                                                                                                                                                         |  |
| 21                                                         | General / Functional | Must support 16 WLANs per AP for SSID deployment flexibility.                                                                                                                                                          |  |
| 22                                                         | General / Functional | Access Point Must continue serving clients when link to controller is down. It should also have option to authenticate user through Radius server directly from Access Point during link unavailability to controller. |  |
| 23                                                         | General / Functional | Must support telnet and/or SSH login to APs directly for troubleshooting flexibility.                                                                                                                                  |  |
| 24                                                         | General / Functional | 802.11e and WMM                                                                                                                                                                                                        |  |
| 25                                                         | General / Functional | Must support QoS and Video Call Admission Control capabilities.                                                                                                                                                        |  |
| 26                                                         | General / Functional | Access point should be able to steer client towards 6 GHz through 802.11v                                                                                                                                              |  |
| 27                                                         | General / Functional | Access point should ensure hardware and software authenticity to provide strong defense against man-in-the-middle attacks for software and firmware                                                                    |  |
| 28                                                         | General / Functional | Access Point must continue serving clients when link to controller is down. It should also have option to authenticate user through Radius server directly from Access Point during link unavailability to controller. |  |
| 29                                                         | General / Functional | Access point should be support 802.11i (WPA2, WPA3), 802.1x/802.1x - SHA256, Enhanced Open/OWE, AES-GCMP256 and CCMP256 security compliant.                                                                            |  |
| 30                                                         | General / Functional | Access point should support EAP-TLS, EAP-TTLS/MSCHAPv2, PEAP and EAP-FAST, AAA Override, Radius profiling                                                                                                              |  |
| 31                                                         | General / Functional | Access point should be Wi-fi alliance certified for Wi-Fi 7 (R1), Wi-Fi 6 (R2), Wi-Fi 6E, WPA3-R3, WPA3-Suite B, Enhanced Open Security and Bluetooth SIG                                                              |  |
| 32                                                         | General / Functional | Access point should be complied for EN 300 328, EN 303 687, EN 50385, EN 55032, EN 55035, EN 61000-6-1                                                                                                                 |  |
| <b>Item Code : A-8</b>                                     |                      |                                                                                                                                                                                                                        |  |
| <b>Name of Item : Standard Indoor Wi-Fi 7 Access Point</b> |                      |                                                                                                                                                                                                                        |  |
| <b>Approved/Eligible OEMs : Cisco, HPE Aruba, Ruckus</b>   |                      |                                                                                                                                                                                                                        |  |

| Sr. No. | Section              | Technical Specification                                                                                                                       | Compliance (Yes/No) |
|---------|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| 1       | General / Functional | Access point should be IEEE 802.11a/b/g/n/ac/ax/be compliant                                                                                  |                     |
| 2       | General / Functional | Access Point shall support 2x2:2 MIMO on all three radio interfaces i.e 2.4ghz, 5ghz and 6ghz.                                                |                     |
| 3       | General / Functional | Access point should support Multiuser Multiple-Input, Multiple-Output (MU-MIMO) for simultaneous uplink and downlink connections.             |                     |
| 4       | General / Functional | Access point should also support latest WiFi 7 technologies like MLO and Preamble Puncturing                                                  |                     |
| 5       | General / Functional | Access Point should have inbuilt Bluetooth radio to support use cases of location, asset tracking and analytics.                              |                     |
| 6       | General / Functional | Access Point shall be able to be powered up using 802.3at power with full 2x2 radio operation on all 3 radios - 2.4ghz, 5 ghz & 6 ghz radio.  |                     |
| 7       | General / Functional | Access Point should support upto 4K-QAM, A-MPDU, A-MSDU, 802.11 DFS, MRC, beamforming, CSD                                                    |                     |
| 8       | General / Functional | Access Point should have 1x 100M/1000M/2.5G Multigigabit Ethernet (RJ-45)                                                                     |                     |
| 9       | General / Functional | Access Point should have USB port for future requirement.                                                                                     |                     |
| 10      | General / Functional | Must have atleast 4 dBi Antenna gain on each client serving radios                                                                            |                     |
| 11      | General / Functional | Access point should have capability to support data rate upto 9 gbps.                                                                         |                     |
| 12      | General / Functional | Must support minimum of 20dbm of transmit power in all 2.4Ghz, 5Ghz & 6ghz radios, and should follow the local regulatory Norms.              |                     |
| 13      | General / Functional | Must support AP enforced load-balance between 2.4Ghz and 5Ghz band.                                                                           |                     |
| 14      | General / Functional | Must incorporate radio resource management for power, channel and performance optimization                                                    |                     |
| 15      | General / Functional | Must support Proactive Key Caching and/or other methods for Fast Secure Roaming.                                                              |                     |
| 16      | General / Functional | Must support Management Frame Protection.                                                                                                     |                     |
| 17      | General / Functional | Should support locally-significant certificates on the APs using a Public Key Infrastructure (PKI).                                           |                     |
| 18      | General / Functional | Must support 16 WLANs per AP for SSID deployment flexibility.                                                                                 |                     |
| 19      | General / Functional | Access Points must support Hardware-based encrypted user data and management traffic between controller and Access point for better security. |                     |
| 20      | General / Functional | Must support the ability to serve clients and monitor the RF environment concurrently.                                                        |                     |
| 21      | General / Functional | Same model AP that serves clients must be able to be dedicated to monitoring the RF environment.                                              |                     |

|    |                      |                                                                                                                                                                                                                        |  |
|----|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 22 | General / Functional | Access point should support 802.11e and WMM                                                                                                                                                                            |  |
| 23 | General / Functional | Access Point should support Per-User and Per-SSID Bandwidth Contract                                                                                                                                                   |  |
| 24 | General / Functional | Should support Application visibility, QoS and Video Call Admission Control capabilities.                                                                                                                              |  |
| 25 | General / Functional | Must support telnet and/or SSH login to APs directly for troubleshooting flexibility.                                                                                                                                  |  |
| 26 | General / Functional | Must be plenum-rated (UL 2043).                                                                                                                                                                                        |  |
| 27 | General / Functional | Access point should ensure hardware and software authenticity to provide strong defense against man-in-the-middle attacks for software and firmware                                                                    |  |
| 28 | General / Functional | Access Point must continue serving clients when link to controller is down. It should also have option to authenticate user through Radius server directly from Access Point during link unavailability to controller. |  |
| 29 | General / Functional | Access point should be support 802.11i (WPA2, WPA3), 802.1x/802.1x - SHA256, Enhanced Open/OWE, AES-GCMP256 and CCMP256 security compliant.                                                                            |  |
| 30 | General / Functional | Access point should support EAP-TLS, EAP-TTLS/MSCHAPv2, PEAP and EAP-FAST, AAA Override, Radius profiling                                                                                                              |  |
| 31 | General / Functional | Access point should be Wi-fi alliance certified for Wi-Fi 7, Wi-Fi 6, Wi-Fi 6E, WPA3-R3, WPA3-Suite B, Enhanced Open Security and Bluetooth SIG                                                                        |  |
| 32 | General / Functional | Access point should be complied for EN 300 328, EN 303 687, EN 50385, EN 55032, EN 55035, EN 61000-6-1                                                                                                                 |  |

**Item Code : A-9**

**Name of Item : Ruggedized Outdoor Wireless Access Point**

**Approved/Eligible OEMs : Cisco, HPE Aruba, Ruckus**

| Sr. No. | Section              | Technical Specification                                                                                                                                                                                                                                           | Compliance (Yes/No) |
|---------|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| 1       | General / Functional | Wireless device proposed must include two band radios 5 GHz and 5/6Ghz, Outdoor (IP67 rated or better) with Wi-Fi6 802.11ax technology                                                                                                                            |                     |
| 2       | General / Functional | The outdoor AP shall provide at least one multigigabit Ethernet interface supporting IEEE 802.3at/802.3bt PoE. A fibre/SFP interface may be offered where required by the approved site design; otherwise an external industrial media converter may be proposed. |                     |
| 3       | General / Functional | The outdoor AP shall provide high-capacity MIMO operation on the supported 5 GHz and/or 6 GHz radios, with integrated omnidirectional antennas or equivalent antennas suited to the approved RF design.                                                           |                     |
| 4       | General / Functional | The AP shall support concurrent dual-band/tri-band operation or an equivalent flexible-radio architecture suitable for the approved outdoor RF design.                                                                                                            |                     |
| 5       | General / Functional | Should have dedicated radio for monitoring air space to perform advanced RF spectrum analysis                                                                                                                                                                     |                     |

|    |                      |                                                                                                                                                                                                                                                                                                |  |
|----|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 6  | General / Functional | The wireless transceiver shall fully support 802.1Q VLAN tagging. It shall support hybrid port-based and MAC-based VLAN tagging.                                                                                                                                                               |  |
| 7  | General / Functional | The wireless transceiver shall not be visible to standard 802.11-enabled devices.                                                                                                                                                                                                              |  |
| 8  | General / Functional | The wireless transceiver shall support 128-bit AES encryption at the link level.                                                                                                                                                                                                               |  |
| 9  | General / Functional | Application hosting/container capability on the AP may be offered as an optional value-added feature and shall not be mandatory for technical eligibility.                                                                                                                                     |  |
| 10 | General / Functional | A built in optional GNSS (Global Navigation Satellite System) receiver should be there to provide coordinates to track the location of the access point in future                                                                                                                              |  |
| 11 | General / Functional | The outdoor AP shall comply with applicable IEC/EN safety, EMC, environmental and radio regulations for deployment in India, including IP66/IP67 or better ingress protection. Railway-specific standards shall apply only where the equipment is deployed in a railway environment.           |  |
| 12 | General / Functional | All wireless transceivers shall support End-to-end QoS that allows advanced traffic engineering. The wireless transceivers shall comply with 8-bit Differentiated Services computer network (DSCP). Wireless transceivers shall guarantee QoS end-to-end in mobility and roaming applications. |  |
| 13 | General / Functional | The wireless transceivers shall be monitored using any SNMP compatible OSS platform, and it shall be possible to export a detailed MIB set which fully characterizes the network behaviors.                                                                                                    |  |
| 14 | General / Functional | All the wireless transceivers shall be remotely manageable through a password protected HTTPS web-interface and an SSH command line interface. Both interfaces are accessible locally at the unit, and remotely over the network.                                                              |  |
| 15 | General / Functional | Operating temperature of the Wireless devices should be -40° to +158°F (-40° to +70°C)                                                                                                                                                                                                         |  |

**Item Code : A-10**

**Name of Item : High-Density Wi-Fi 7 Access Point**

**Approved/Eligible OEMs : Cisco, HPE Aruba, Ruckus**

| Sr. No. | Section              | Technical Specification                                                                                                                                                                                                                                                             | Compliance (Yes/No) |
|---------|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| 1       | General / Functional | The high-density AP shall be Wi-Fi 7 and support Quad Radio operation on concurrent 2.4 GHz, 5 GHz and 6 GHz band with 4x4 MIMO on the principal high-capacity bands, or an equivalent/higher aggregate-capacity radio design. MU-MIMO and Multi-Link Operation shall be supported. |                     |

|    |                      |                                                                                                                                                                                                                                                    |  |
|----|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 2  | General / Functional | The AP shall include integrated BLE and/or IEEE 802.15.4 IoT capability. GNSS or equivalent location enhancement may be offered where available.                                                                                                   |  |
| 3  | General / Functional | Access Point shall be able to powered up using 802.3at power.                                                                                                                                                                                      |  |
| 4  | General / Functional | The AP shall support flexible radio operation or an equivalent automated mechanism for optimizing use of the 2.4 GHz, 5 GHz and 6 GHz bands in a high-density environment.                                                                         |  |
| 5  | General / Functional | The wireless solution shall provide dedicated or time-sliced spectrum analysis, WIDS/WIPS and off-channel RF monitoring without materially affecting client service.                                                                               |  |
| 6  | General / Functional | AP-hosted IoT applications/containers may be offered as an optional value-added capability; standards-based IoT integration through BLE/802.15.4, APIs or gateways shall be acceptable.                                                            |  |
| 7  | General / Functional | The AP shall provide at least one multigigabit Ethernet uplink appropriate to its maximum practical throughput; dual uplinks may be provided for resiliency or link aggregation. The bidder shall state supported speeds and redundancy behaviour. |  |
| 8  | General / Functional | Access Point should have USB port for future requirement.                                                                                                                                                                                          |  |
| 9  | General / Functional | Must have atleast 6 dBi inbuilt Antenna gain on each radios with option to adjust antenna beam.                                                                                                                                                    |  |
| 10 | General / Functional | The AP shall provide an aggregate maximum PHY rate appropriate to the high-density design and not less than 10 Gbps. The bidder shall state per-band and aggregate PHY rates.                                                                      |  |
| 11 | General / Functional | Must support AP enforced load-balance between 2.4Ghz and 5Ghz band.                                                                                                                                                                                |  |
| 12 | General / Functional | Must incorporate radio resource management for power, channel and performance optimization                                                                                                                                                         |  |
| 13 | General / Functional | Must have -93 dB or better Receiver Sensitivity.                                                                                                                                                                                                   |  |
| 14 | General / Functional | Must support Proactive Key Caching and/or other methods for Fast Secure Roaming.                                                                                                                                                                   |  |
| 15 | General / Functional | Must support Management Frame Protection.                                                                                                                                                                                                          |  |
| 16 | General / Functional | Should support locally-significant certificates on the APs using a Public Key Infrastructure (PKI).                                                                                                                                                |  |
| 17 | General / Functional | Access Points must support Hardware-based encrypted user data and management traffic between controller and Access point for better security.                                                                                                      |  |
| 18 | General / Functional | Must support the ability to serve clients and monitor the RF environment concurrently.                                                                                                                                                             |  |
| 19 | General / Functional | Same model AP that serves clients must be able to be dedicated to monitoring the RF environment.                                                                                                                                                   |  |
| 20 | General / Functional | The Access point shall be IP67 rated                                                                                                                                                                                                               |  |

| 21                                                                             | General / Functional | Must support 16 WLANs per AP for SSID deployment flexibility.                                                                                                                                                                                                                                                      |                            |
|--------------------------------------------------------------------------------|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| 22                                                                             | General / Functional | Access Point Must continue serving clients when link to controller is down. It should also have option to authenticate user through Radius server directly from Access Point during link unavailability to controller.                                                                                             |                            |
| 23                                                                             | General / Functional | Must support telnet and/or SSH login to APs directly for troubleshooting flexibility.                                                                                                                                                                                                                              |                            |
| 24                                                                             | General / Functional | 802.11e and WMM                                                                                                                                                                                                                                                                                                    |                            |
| 25                                                                             | General / Functional | Must support QoS and Video Call Admission Control capabilities.                                                                                                                                                                                                                                                    |                            |
| 26                                                                             | General / Functional | Access point should be Wifi alliance certified for Wifi-7, Wi-Fi 6 (R2), Wi-Fi 6E, WPA3-R3, WPA3-Suite B and Bluetooth SIG for Bluetooth low energy.                                                                                                                                                               |                            |
| <b>Item Code : A-11</b>                                                        |                      |                                                                                                                                                                                                                                                                                                                    |                            |
| <b>Name of Item : Centralized SDN Controller and Network Management System</b> |                      |                                                                                                                                                                                                                                                                                                                    |                            |
| <b>Approved/Eligible OEMs : Cisco, HPE Aruba, Ruckus</b>                       |                      |                                                                                                                                                                                                                                                                                                                    |                            |
| <b>Sr. No.</b>                                                                 | <b>Section</b>       | <b>Technical Specification</b>                                                                                                                                                                                                                                                                                     | <b>Compliance (Yes/No)</b> |
| 1                                                                              | General / Functional | Management Solution be comprehensive solution to manage, visualize and monitor the network from a single graphical interface for wired and wireless network devices.                                                                                                                                               |                            |
| 2                                                                              | General / Functional | The management solution may be delivered as an OEM physical appliance, virtual appliance, on-premises software platform or cloud-managed service, subject to the RFP's security, availability and data-residency requirements. It shall be sized for the specified estate and include HA/redundancy as applicable. |                            |
| 3                                                                              | General / Functional | The management solution shall be scalable to manage at least 1,500 switches/controllers or gateways and 3,000 APs, either on the proposed instance/cluster or through a documented scale-out architecture included in the solution.                                                                                |                            |
| 4                                                                              | General / Functional | Management Controller should be able to monitor 40,000 concurrent endpoints on the network                                                                                                                                                                                                                         |                            |
| 5                                                                              | General / Functional | For a physical appliance, standard console and service interfaces shall be provided. For virtual or cloud deployment, equivalent secure console, backup and recovery mechanisms shall be available.                                                                                                                |                            |
| 6                                                                              | General / Functional | The Management solution should be able to provide redundancy within the same Location or across 2 locations                                                                                                                                                                                                        |                            |
| 7                                                                              | General / Functional | Switches and Wireless network devices and management solution should be from same OEM                                                                                                                                                                                                                              |                            |
| 8                                                                              | General / Functional | Proposed solution should allow admin to manage network in a hierarchical fashion by adding areas and buildings based on geographic location of the campus network                                                                                                                                                  |                            |

|    |                      |                                                                                                                                                                                                    |  |
|----|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 9  | General / Functional | Controller should be able to integrate with NAC solution to provide integrated security.                                                                                                           |  |
| 10 | General / Functional | The solution should have support for standard southbound protocols that enables it to communicate with breadth of network devices                                                                  |  |
| 11 | General / Functional | The solution should have open APIs to create intelligent, open, programmable network to build advanced automation services                                                                         |  |
| 12 | General / Functional | Solution should support for TACACS based authentication                                                                                                                                            |  |
| 13 | General / Functional | Solution should support for standard local authentication                                                                                                                                          |  |
| 14 | General / Functional | Solution should support for Radius based authentication                                                                                                                                            |  |
| 15 | General / Functional | The solution shall provide at least 3 levels of access - read, write and super administrator.                                                                                                      |  |
| 16 | General / Functional | Proposed solution should supports Representational State Transfer (REST) APIs at the northbound layer for programmability                                                                          |  |
| 17 | General / Functional | Network management tool should support multiple protocols to retrieve the network information                                                                                                      |  |
| 18 | General / Functional | Solution should support multiple credentials for the devices to be discovered                                                                                                                      |  |
| 19 | General / Functional | The management solution should auto discover the network elements as well as their current status.                                                                                                 |  |
| 20 | General / Functional | Management solution should have the ability to add network devices into inventory via import from a comma-separated variable (CSV) file, manual add or via API                                     |  |
| 21 | General / Functional | The network management solution should standardize baseline configuration across the campus.                                                                                                       |  |
| 22 | General / Functional | Network management solution should have RF coverage planning tool.                                                                                                                                 |  |
| 23 | General / Functional | Network automation solution should discover IPV6 enabled devices                                                                                                                                   |  |
| 24 | General / Functional | The network management solution should have a workflow built with configurations which can be deployed across multiple devices and device types.                                                   |  |
| 25 | General / Functional | The solution should provide option to upgrade or downgrade the device during the zero-touch provisioning, as per the administrator assigned software version, before bringing it into the network. |  |
| 26 | General / Functional | The management solution shall have the ability to compare configuration versions using a side-by-side, split-screen display to highlight differences between current and captured configuration    |  |
| 27 | General / Functional | The network management solution should be able to embed networking best practices to proactively identify configuration settings contradicting to baselines configuration prior to deployment.     |  |

|    |                      |                                                                                                                                                                                                                                                                                                 |  |
|----|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 28 | General / Functional | Proposed management solution should provide centralized policy creation for configuring each type of device across the network                                                                                                                                                                  |  |
| 29 | General / Functional | Solution should have capabilities to monitor the health of network devices including CPU & memory utilization, link errors & discards and link availability (Real time and trending)                                                                                                            |  |
| 30 | General / Functional | Solution should have self learning capabilities like discovering the devices, getting devices onboarded using zero-touch provisioning or equivalent automated onboarding and creating a topology automatically with details like device health, link health, Hostname and management IP address |  |
| 31 | General / Functional | Solution should provide complete inventory of network devices along with firmware details.                                                                                                                                                                                                      |  |
| 32 | General / Functional | Proposed solution should be able to display the current running configuration of the network device                                                                                                                                                                                             |  |
| 33 | General / Functional | The system must support device configuration backup in manual or scheduled basis.                                                                                                                                                                                                               |  |
| 34 | General / Functional | The network management solution should recommended latest/stable software images                                                                                                                                                                                                                |  |
| 35 | General / Functional | The solution shall have a provision to monitor the scheduled device software image upgrade changes for failure                                                                                                                                                                                  |  |
| 36 | General / Functional | The solution shall have the ability to detect manual configuration changes to network devices                                                                                                                                                                                                   |  |
| 37 | General / Functional | The solution should perform Pre-upgrade checks and Post-upgrade checks                                                                                                                                                                                                                          |  |
| 38 | General / Functional | Solution should have the capability to perform software image upgrade for multiple devices at once.                                                                                                                                                                                             |  |
| 39 | General / Functional | The solution should have the capability to activate the image later based on the network conditions                                                                                                                                                                                             |  |
| 40 | General / Functional | The automation tool should provide compliance for software version report per site                                                                                                                                                                                                              |  |
| 41 | General / Functional | Solution provides the ability to view license usage.                                                                                                                                                                                                                                            |  |
| 42 | General / Functional | Solution sends alerts prior to license expiry.                                                                                                                                                                                                                                                  |  |
| 43 | General / Functional | Solution has the ability to report license consumption.                                                                                                                                                                                                                                         |  |
| 44 | General / Functional | Solution should allow to create common base configuration templates for a group of managed devices at a site or a group of sites.                                                                                                                                                               |  |
| 45 | General / Functional | Solution should be able to automate and schedule image upgrade for both for wired and wireless networks with none to minimal network impact.                                                                                                                                                    |  |
| 46 | General / Functional | Solution should provide Compliance against following - Configuration, Firmware and Security Vulnerability                                                                                                                                                                                       |  |

|    |                      |                                                                                                                                                                                                                                                                          |  |
|----|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 47 | General / Functional | Solution should provide Firmware compliance while comparing with corporate standardized image for the switching models                                                                                                                                                   |  |
| 48 | General / Functional | The solution should provide customizable configuration templates based on validated designs and guided workflows                                                                                                                                                         |  |
| 49 | General / Functional | Solution should have capability to connect with OEM cloud to Auto Update/Download the open security vulnerabilities against devices firmware and remediation in terms of firmware or patch update under security advisories to fix the vulnerability on network devices. |  |
| 50 | General / Functional | Administrator should have the ability to run batch CLI commands to the managed devices from network management dashboard directly, without logging into each device individually.                                                                                        |  |
| 51 | General / Functional | Solution should have the ability of adding 3rd party devices without Licensing check                                                                                                                                                                                     |  |
| 52 | General / Functional | Solution should support physical branch provisioning by automating onboarding, initial configuration, and customer-supplied configurations for the complete branch network.                                                                                              |  |
| 53 | General / Functional | Should have the capability to monitor and troubleshoot the proactive and predictive aspects of running a network and ensuring optimal client, application, and service performance                                                                                       |  |
| 54 | General / Functional | The management solution should auto discover the network elements as well as their current status.                                                                                                                                                                       |  |
| 55 | General / Functional | Management Solution should provide capability to correlate multiple Key Performance Indicators (KPIs) to determine the root cause of a problem                                                                                                                           |  |
| 56 | General / Functional | Management solution should have capability to provide in-depth health scores for a network and its devices, clients, applications, and services.                                                                                                                         |  |
| 57 | General / Functional | The solution shall use standards-based mechanisms such as LLDP, SNMP, ARP/ND, MAC tables, APIs and device tracking for topology and endpoint discovery. Proprietary discovery protocols may additionally be supported but shall not be mandatory.                        |  |
| 58 | General / Functional | Solution should be able to integrate with AAA, SNMP, SYSLOG, DHCP and DNS Servers etc.to capture the network telemetry data.                                                                                                                                             |  |
| 59 | General / Functional | Solution should have capabilities to alert/alarm the IT team when the issue is detected over the network e.g. reachability issues, device health, link utilization and network issues etc. and it should be categorized against criticality on the dashboard             |  |
| 60 | General / Functional | The solution should provide notification/alert in case of network related health issues                                                                                                                                                                                  |  |
| 61 | General / Functional | The management tool should diagnose client and application issues using recent and historical data.                                                                                                                                                                      |  |

|    |                      |                                                                                                                                                                         |  |
|----|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 62 | General / Functional | The solution shall provide at-a-glance fault summary dashboards to view top unhealthy network elements with status KPIs and drill down to view the detailed information |  |
| 63 | General / Functional | The management solution should identify top network issues to delivers an understanding of which faults to investigate first                                            |  |
| 64 | General / Functional | The management solution should support Web-based location-specific dashboards to summarize network health at-a-glance.                                                  |  |
| 65 | General / Functional | Applications or flows collected on the management solution have to be recognized and categorized accordingly                                                            |  |
| 66 | General / Functional | Operations staff should be able to search for users based on readily available attributes, e.g., username, MAC or IP address.                                           |  |
| 67 | General / Functional | The management solution should support custom Qos Profiles for different classes                                                                                        |  |
| 68 | General / Functional | The centralized management solution should provide the capability to enable captures from the UI itself                                                                 |  |
| 69 | General / Functional | Solution should support the capability to create dynamic baseline for different client onboarding KPIs                                                                  |  |
| 70 | General / Functional | Solution should support the capability to generate issues based on dynamic baseline for different client onboarding KPIs                                                |  |
| 71 | General / Functional | The solution shall be able to provide a high level and drill down reporting views of the status of network environment.                                                 |  |

**Name of Item : A-12**

**Name of Item : Network Access Control (NAC) Solution**

**Approved/Eligible OEMs : Cisco, HPE Aruba, Ruckus**

| Sr. No. | Section              | Technical Specification                                                                                                                                                                                                                       | Compliance (Yes/No) |
|---------|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| 1       | General / Functional | The Solution should provide a highly powerful and flexible attribute-based access control solution that combines authentication, authorization, and accounting (AAA); posture; profiling; and guest management services on a single platform. |                     |
| 2       | General / Functional | It should allow enterprises to authenticate and authorize users and endpoints via wired, wireless, and VPN with consistent policy throughout the enterprise                                                                                   |                     |
| 3       | General / Functional | Provides complete guest lifecycle management by empowering sponsors to on-board guests.                                                                                                                                                       |                     |
| 4       | General / Functional | Solution should be scalable enough to support 30000 endpoints in the network with additional licenses whenever needed.                                                                                                                        |                     |
| 5       | General / Functional | Solution should support 25000 users from day 1                                                                                                                                                                                                |                     |

|    |                      |                                                                                                                                                                                                                                                                          |  |
|----|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 6  | General / Functional | Delivers customizable self service portals as well as the ability to host custom web pages to ease device and guest on-boarding, automate endpoint secure access and service provisioning, and enhance the overall end-user experience inside business-defined workflows |  |
| 7  | General / Functional | The NAC solution shall support guest onboarding through configurable self-registration, OTP/email/SMS verification, sponsor approval and/or federated identity providers, as permitted by the purchaser's security policy.                                               |  |
| 8  | General / Functional | The solution should support sponsor approval for guest users connecting into the network and the approval request should have control from multiple sponsor to avoid single point of failure                                                                             |  |
| 9  | General / Functional | The solution should support flexible guest account approval even in absence of sponsor                                                                                                                                                                                   |  |
| 10 | General / Functional | The Solution should support complete guest lifecycle where Sponsor should be able to Extend,Suspend and reinstate guest accounts with reasons.                                                                                                                           |  |
| 11 | General / Functional | Offers comprehensive visibility of the network by automatically discovering, classifying, and controlling endpoints connected to the network to enable the appropriate services per endpoint                                                                             |  |
| 12 | General / Functional | Enforces security policies by blocking, isolating, and repairing noncompliant machines in a quarantine area without requiring administrator attention                                                                                                                    |  |
| 13 | General / Functional | Offers a built-in monitoring, reporting, and troubleshooting console to assist helpdesk operators and administrators streamline operations                                                                                                                               |  |
| 14 | General / Functional | Allows you to get finer granularity while identifying devices on your network with Active Endpoint Scanning                                                                                                                                                              |  |
| 15 | General / Functional | The NAC solution should be able to block unauthenticated/rogue machine without giving any access to the network.                                                                                                                                                         |  |
| 16 | General / Functional | Augments network-based profiling by targeting specific endpoints (based on policy) for specific attribute device scans, resulting in higher accuracy and comprehensive visibility of what is on your network                                                             |  |
| 17 | General / Functional | The NAC solution should be able to control the user even before IP address is assigned. It should act as a pre-admission solution                                                                                                                                        |  |
| 18 | General / Functional | The NAC solution should be able to integrate with APT, NBAD and SIEM solution                                                                                                                                                                                            |  |
| 19 | General / Functional | The solution should provide full TACACS+ capability including enable password, configuration present for different NAD types, TACACS+ proxy etc.                                                                                                                         |  |
| 20 | General / Functional | Manages endpoint access to the network with the Endpoint Protection Service, which enables administrators to specify an endpoint and select an action - for example, move to a new VLAN, return to the                                                                   |  |

|    |                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |  |
|----|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
|    |                      | original VLAN, or isolate the endpoint from the network entirely - all in a simple interface                                                                                                                                                                                                                                                                                                                                                                          |  |
| 21 | General / Functional | Utilizes standard RADIUS protocol for authentication, authorization, and accounting (AAA).                                                                                                                                                                                                                                                                                                                                                                            |  |
| 22 | General / Functional | Supports a wide range of authentication protocols, including PAP, MS-CHAP, Extensible Authentication Protocol (EAP)-MD5, Protected EAP (PEAP), EAP-Flexible Authentication via Secure Tunneling (FAST), and EAP-Transport Layer Security (TLS).                                                                                                                                                                                                                       |  |
| 23 | General / Functional | Offers a rules-based, attribute-driven policy model for creating flexible and business-relevant access control policies. Provides the ability to create fine-grained policies by pulling attributes from predefined dictionaries that include information about user and endpoint identity, posture validation, authentication protocols, profiling identity, or other external attribute sources. Attributes can also be created dynamically and saved for later use |  |
| 24 | General / Functional | Provides a wide range of access control mechanisms, including downloadable access control lists (dACLs), VLAN assignments, URL redirect, and role-/security-group-based tagging or an equivalent policy-enforcement mechanism.                                                                                                                                                                                                                                        |  |
| 25 | General / Functional | Should have predefined device templates for a wide range of endpoints, such as IP phones, printers, IP cameras, smartphones, and tablets.                                                                                                                                                                                                                                                                                                                             |  |
| 26 | General / Functional | It should allow Administrators to create their own device templates. These templates can be used to automatically detect, classify, and associate administrative-defined identities when endpoints connect to the network. Administrators can also associate endpoint-specific authorization policies based on device type.                                                                                                                                           |  |
| 27 | General / Functional | Solution must allow administrator to add exception for certain device properties in the device templates/ device profiles available in the solution to filter unintentionally picked parameters of endpoints.                                                                                                                                                                                                                                                         |  |
| 28 | General / Functional | The Solution should have capability to collect endpoint attribute data via passive network telemetry, querying the actual endpoints, or alternatively from the infrastructure via device sensors on switches.                                                                                                                                                                                                                                                         |  |
| 29 | General / Functional | The Solution should have capability to see endpoints attribute data via passive network telemetry or alternatively from the infrastructure via device sensors on switches at Core, Distribution and Access Layer.                                                                                                                                                                                                                                                     |  |
| 30 | General / Functional | Solution should allow end users to interact with a self-service portal for device on-boarding, providing a registration vehicle for all types of devices as well as automatic supplicant provisioning and certificate                                                                                                                                                                                                                                                 |  |

|    |                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |  |
|----|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
|    |                      | enrollment for standard PC and mobile computing platforms.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |  |
| 31 | General / Functional | Should support full guest lifecycle management, whereby guest users can access the network for a limited time, either through administrator sponsorship or by self-signing via a guest portal. Allows administrators to customize portals and policies based on specific needs of the enterprise.                                                                                                                                                                                                                                                                                                                                                                         |  |
| 32 | General / Functional | Verifies endpoint posture assessment for PCs connecting to the network. Works via either a persistent client-based agent or a temporal web agent to validate that an endpoint is conforming to a company's posture policies. Provides the ability to create powerful policies that include but are not limited to checks for the latest OS patches, antivirus and antispymware software packages with current definition file variables (version, date, etc.), registries (key, value, etc), and applications. Solution should support auto-remediation of PC clients as well as periodic reassessment to make sure the endpoint is not in violation of company policies. |  |
| 33 | General / Functional | Allows administrators to quickly take corrective action (Quarantine, Un-Quarantine, or Shutdown) on risk-compromised endpoints within the network. This helps to reduce risk and increase security in the network.                                                                                                                                                                                                                                                                                                                                                                                                                                                        |  |
| 34 | General / Functional | Enables administrators to centrally configure and manage profiler, posture, guest, authentication, and authorization services in a single web-based GUI console, greatly simplifying administration by providing consistency in managing all these services.                                                                                                                                                                                                                                                                                                                                                                                                              |  |
| 35 | General / Functional | Includes a built-in web console for monitoring, reporting, and troubleshooting to assist help-desk and network operators in quickly identifying and resolving issues. Offers comprehensive historical and real-time reporting for all services, logging of all activities, and real-time dashboard metrics of all users and endpoints connecting to the network.                                                                                                                                                                                                                                                                                                          |  |
| 36 | General / Functional | Should support consistent policy in centralized and distributed deployments that allows services to be delivered where they are needed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |  |
| 37 | General / Functional | Solution should have capability to determine whether users are accessing the network on an authorized, policy-compliant device.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |  |
| 38 | General / Functional | Solution should have capability to establish user identity, location, and access history, which can be used for compliance and reporting.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |  |
| 39 | General / Functional | Solution should have capability to assign services based on the assigned user role, group, and associated policy (job role, location, device type, and so on).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |  |

|    |                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |  |
|----|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 40 | General / Functional | Solution should have capability to grant authenticated users with access to specific segments of the network, or specific applications and services, or both, based on authentication results.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |  |
| 41 | General / Functional | Solution should have capability which allows users to add a device on a portal, where the device goes through a registration process for network access. Should allow users to mark as lost any device that you have registered in the network, and blacklist the device on the network, which prevents others from unauthorized network access when using the blacklisted device. Should have capability to reinstate a blacklisted device to its previous status in Device Portal, and regain network access without having to register the device again in the Devices Portal. Should also support removing any device in the enterprise network temporarily, then register the device for network access again later. |  |
| 42 | General / Functional | Should provide a Registered Endpoints Report which provides information about a list of endpoints that are registered through the device registration portal by a specific user for a selected period of time. The report should provide the following details •Logged in Date and Time •Portal User (who registered the device) •MAC Address •Identity Group •Endpoint Policy •Static Assignment •Static Group Assignment •Endpoint Policy ID •NMAP Subnet Scan ID •Device Registration Status                                                                                                                                                                                                                           |  |
| 43 | General / Functional | Solution should classify a client machine, and should support client provisioning resource policies to ensure that the client machine is set up with an appropriate agent version, up-to-date compliance modules for antivirus and antispymware vendor support, and correct agent customization packages and profiles, if necessary                                                                                                                                                                                                                                                                                                                                                                                       |  |
| 44 | General / Functional | Solution should support automatic provisioning of NAC agents                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |  |
| 45 | General / Functional | The NAC solution should support any SAML v2 compliant solution.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |  |
| 46 | General / Functional | Solution should support periodic reassessment for clients that are already successfully postured for compliance.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |  |
| 47 | General / Functional | Solution should support the following endpoint checks for compliance for windows endpoints: - Check operating system/service packs/hotfixes - Check process, registry, file & application - Check for Antivirus installation/Version/ Antivirus Definition Date - Check for Antispymware installation/Version/ Antispymware Definition Date - Check for windows update running & configuration                                                                                                                                                                                                                                                                                                                            |  |

|    |                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |  |
|----|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 48 | General / Functional | Solution should support following remediation options for windows endpoints: - File remediation to allow clients download the required file version for compliance - Link remediation to allow clients to click a URL to access a remediation page or resource - Antivirus remediation to update clients with up-to-date file definitions for compliance after remediation. - Antispyware remediation to update clients with up-to-date file definitions for compliance after remediation. - Launch program remediation for NAC Agent to remediate clients by launching one or more applications for compliance. - Windows update remediation to ensure Automatic Updates configuration is turned on Windows clients per security policy. |  |
| 49 | General / Functional | The NAC solution shall integrate through supported APIs or standard interfaces with leading UEM/MDM platforms, including at least two currently supported enterprise UEM products. The bidder shall list validated integrations and versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |  |
| 50 | General / Functional | Solution should support configuring MDM policy based on the attributes lie: DeviceRegisterStatus, DeviceCompliantStatus, DiskEncryptionStatus, PinLockStatus, JailBrokenStatus, SerialNumber, Manufacturer, IMEI, OsVersion & phone number, etc                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |  |
| 51 | General / Functional | Solution should support receiving updated endpoint profiling policies and the updated OUI database as a feed from the OEM database.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |  |
| 52 | General / Functional | The solution should provide facility to control where mobile devices are allowed on the network, based on the device type, operating system, owner of the device and user login credentials.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |  |
| 53 | General / Functional | Should support native supplicant profiles to enable users to bring their own devices into network. When the user logs in, based on the profile that you associate with that user's authorization requirements, solution should provide the necessary supplicant provisioning wizard needed to set up the user's personal device to access the network. This should be supported over Microsoft windows, Apple Mac and iOS and Android devices.                                                                                                                                                                                                                                                                                            |  |
| 54 | General / Functional | When endpoints are discovered on the network, they can be profiled dynamically based on the configured endpoint profiling policies, and assigned to the matching endpoint identity groups depending on their profiles.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |  |
| 55 | General / Functional | Should support using a simple filter that you can use to filter endpoints. The quick filter filters endpoints based on field descriptions, such as the endpoint profile, MAC address, and the static status that is assigned to endpoints when they are created in the Endpoints page.                                                                                                                                                                                                                                                                                                                                                                                                                                                    |  |

|    |                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |  |
|----|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 56 | General / Functional | Should support importing endpoints from a comma-separated values (CSV) file in which the list of endpoints appears with the MAC address and the endpoint profiling policy details separated by a comma.                                                                                                                                                                                                                                                                                       |  |
| 57 | General / Functional | Support for importing endpoints from LDAP server. Should allow to import MAC addresses and the associated profiles of endpoints securely from an LDAP server. Should support an LDAP server to import endpoints and the associated profiles, by using either the default port 389, or securely over SSL, by using the default port 636.                                                                                                                                                       |  |
| 58 | General / Functional | Should support multiple Admin Group Roles and responsibilities like HelpDesk Admin, Identity Admin, Monitoring Admin, Network Device Admin, Policy Admin, RBAC Admin, Super Admin and System Admin                                                                                                                                                                                                                                                                                            |  |
| 59 | General / Functional | Should support Role-based access policies which are access control policies which allow you to restrict the network access privileges for any user or group. Role-based access policies are defined when you configure specific access control policies and permissions. These admin access policies allow you to customize the amount and type of access on a per-user or per-group basis using specified role-based access permission settings that apply to a group or an individual user. |  |
| 60 | General / Functional | Should support Identity source sequences which defines the order in which the solution will look for user credentials in the different databases. Solution should support the following databases: •Internal Users •Internal Endpoints •Active Directory •LDAP •RSA •RADIUS Token Servers •Certificate Authentication Profiles                                                                                                                                                                |  |
| 61 | General / Functional | Must be able to differentiate policy based on device type + authentication                                                                                                                                                                                                                                                                                                                                                                                                                    |  |
| 62 | General / Functional | The solution should support BYOD workflow for Partner/Contractor or Employees for BYOD scenario by automatically provisioning the supplicant such that Owner & the device are authenticated based on certificate.                                                                                                                                                                                                                                                                             |  |
| 63 | General / Functional | The NAC solution should be standard RADIUS server with built-in certificate authority                                                                                                                                                                                                                                                                                                                                                                                                         |  |
| 64 | General / Functional | The CA server should be able to provision certificate for multiple use cases like BYOD, EAP authentication and Third Party Client and Server side authentication.                                                                                                                                                                                                                                                                                                                             |  |
| 65 | General / Functional | The solution must have internal CA server functionality with flexibility to create certificate template to be used by other network services                                                                                                                                                                                                                                                                                                                                                  |  |
| 66 | General / Functional | Solution should support MAB and can further utilize identity of the endpoint to apply the proper rules for access. MacAddressBypass is typically used for devices which do not support 802.1x                                                                                                                                                                                                                                                                                                 |  |

|    |                      |                                                                                                                                                                                                                                                                                                                                                                            |  |
|----|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 67 | General / Functional | Solution must support Non 802.1x technology on assigned ports and 802.1x technology on open use ports                                                                                                                                                                                                                                                                      |  |
| 68 | General / Functional | Solution should provide support policy enforcement through VPN gateways                                                                                                                                                                                                                                                                                                    |  |
| 69 | General / Functional | Solution must allow users access to the network in a worst case scenario in case of AAA server outages or any other reasons like WAN failure.                                                                                                                                                                                                                              |  |
| 70 | General / Functional | Should support authenticating Machines and users connected to the same port on the switch in a single authentication flow                                                                                                                                                                                                                                                  |  |
| 71 | General / Functional | Should support authenticating IP phones and users connected behind IP phones on the same physical port.                                                                                                                                                                                                                                                                    |  |
| 72 | General / Functional | The NAC solution shall profile managed and unmanaged/headless endpoints using multiple available data sources such as MAC OUI, DHCP, RADIUS, HTTP/HTTPS metadata, DNS, LLDP/LLDP-MED, SNMP, flow telemetry and mirrored traffic. Equivalent sensors or integrations are acceptable; no single sensor type shall be mandatory where the same profiling outcome is achieved. |  |
| 73 | General / Functional | Soution should support troubleshooting authentication issues by triggering session reauthentication to follow up with an attempt to reauthenticate again.                                                                                                                                                                                                                  |  |
| 74 | General / Functional | The NAC solution should integrate with vulnerability scanner like Rapid7, Tenable etc. Should be a listed vendor and officially supported integration and should allow use of threat intelligence to build authorization permissions based on the vulnerability scores received from these tools to enforce permissions.                                                   |  |
| 75 | General / Functional | Should support session termination with port shutdown option to block an infected host that sends a lot of traffic over the network.                                                                                                                                                                                                                                       |  |
| 76 | General / Functional | Should support the functionality to force endpoint to reacquire IP address that do not support a supplicant or client to generate a DHCP request after a vlan change.                                                                                                                                                                                                      |  |
| 77 | General / Functional | Troubleshooting & Monitoring Tools                                                                                                                                                                                                                                                                                                                                         |  |
| 78 | General / Functional | Should support evaluation of the configuration of the device with the standard configuration.                                                                                                                                                                                                                                                                              |  |
| 79 | General / Functional | Should support TCP dump utility & also support saving a TCP dump file.                                                                                                                                                                                                                                                                                                     |  |
| 80 | General / Functional | Solution should support schedule reports to run and re-run at specific time or time intervals & send and receive email notifications once the reports are generated.                                                                                                                                                                                                       |  |
| 81 | General / Functional | The solution must have internal CA server functionality to provision certificate for multiple use cases like BYOD, Contractor, Employee Asset etc.                                                                                                                                                                                                                         |  |
| 82 | General / Functional | The Solution should support complete guest lifecycle where Sponsor should be able to Extend,Suspend and reinstate guest accounts with reasons.                                                                                                                                                                                                                             |  |

|    |                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |  |
|----|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 83 | General /<br>Functional | The solution should support centralized and distributed deployment options with clustering of nodes or cross-site failover for disaster recovery scenarios                                                                                                                                                                                                                                                                                                                                                        |  |
| 84 | General /<br>Functional | Solution should support integration with leading helpdesk ticketing system. It should support self remediation through end user self support and automatic remediation including guided remediation, quarantine, manual remediation etc.                                                                                                                                                                                                                                                                          |  |
| 85 | General /<br>Functional | Any third party product required to achieve the functionality should be provided with the necessary enterprise version license of software/appliance and necessary hardware, database and other relevant software or hardware etc should be provided with the solution                                                                                                                                                                                                                                            |  |
| 86 | General /<br>Functional | Solutions must support agent, agentless and dissolvable agent method for performing endpoint profiling, baselining, health check and prevention                                                                                                                                                                                                                                                                                                                                                                   |  |
| 87 | General /<br>Functional | Solution should be able to enforce Layer 4 controls right from Access to distribution to core to edge to data center to servers without the need of mirroring the traffic and maintaining end to end segmentation even when two endpoints are in same broadcast domain.                                                                                                                                                                                                                                           |  |
| 88 | General /<br>Functional | Solution should consume license only based on active devices on the network where Devices include user endpoints (such as laptops, tablets and smartphones), non-user devices (such as printers, IP phones, security equipment, medical devices, manufacturing equipment), virtual machines, Network infrastructure devices (such as switches, routers and access points) should not consume license and If so vendor should consider these licenses exclusively and should be counted along with User/Endpoints. |  |
| 89 | General /<br>Functional | Solution should support detecting Endpoint anomaly behavior for example - a device MAC address earlier seen on Wired Network next moment or later seen on Wireless network etc.                                                                                                                                                                                                                                                                                                                                   |  |
| 90 | General /<br>Functional | Open seating environments where the MAC address is not persistent, solution should be to authorize managed endpoint                                                                                                                                                                                                                                                                                                                                                                                               |  |
| 91 | General /<br>Functional | The solution shall identify IoT devices using profiling and, where supported by devices and network infrastructure, Manufacturer Usage Description (MUD) as defined by the IETF or an equivalent standards-based mechanism.                                                                                                                                                                                                                                                                                       |  |

## 10.2 Passive Component:

| Technical Specification: Outdoor Armoured Single Mode Optical Fiber Cable (OS2) – Various Fiber Counts |                                       |                                                                                                                         |
|--------------------------------------------------------------------------------------------------------|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Approved/Eligible OEMs : CommScope/Molex/Legrand                                                       |                                       |                                                                                                                         |
| Sr. No.                                                                                                | Parameter                             | Minimum Technical Specification                                                                                         |
| 1                                                                                                      | Cable Type                            | Outdoor Armoured Single Mode Optical Fiber Cable                                                                        |
| 2                                                                                                      | Fiber Type                            | Single Mode OS2, 9/125 $\mu\text{m}$                                                                                    |
| 3                                                                                                      | Number of Fibers                      | As specified in the BOQ                                                                                                 |
| 4                                                                                                      | Fiber Standard                        | ITU-T G.652.D, backward compatible with ITU-T G.657.A1 or higher                                                        |
| 5                                                                                                      | Cable Construction                    | Central Loose Tube / Multi Loose Tube / Uni-Tube construction as per OEM design suitable for the specified fiber count. |
| 6                                                                                                      | Tube Material                         | OEM Standard                                                                                                            |
| 7                                                                                                      | Water Blocking                        | Water swellable yarn, tape or equivalent OEM technology to prevent longitudinal water ingress                           |
| 8                                                                                                      | Strength Member                       | Glass Yarn / FRP / OEM Standard                                                                                         |
| 9                                                                                                      | Armouring                             | Corrugated Steel Tape Armour (ECCS or equivalent)                                                                       |
| 10                                                                                                     | Rip Cord                              | Required                                                                                                                |
| 11                                                                                                     | Outer Sheath                          | UV Stabilized HDPE, suitable for outdoor installation and underground duct/direct burial applications                   |
| 12                                                                                                     | Sheath Colour                         | OEM Standard                                                                                                            |
| 13                                                                                                     | Applicable Standards                  | IEC 60793, IEC 60794, ISO/IEC 11801, ITU-T G.652.D, RoHS Compliant                                                      |
| 14                                                                                                     | Attenuation @ 1310 nm                 | $\leq 0.35 \text{ dB/km}$                                                                                               |
| 15                                                                                                     | Attenuation @ 1550 nm                 | $\leq 0.22 \text{ dB/km}$                                                                                               |
| 16                                                                                                     | Cable Diameter                        | OEM Standard                                                                                                            |
| 17                                                                                                     | Cable Weight                          | OEM Standard                                                                                                            |
| 18                                                                                                     | Minimum Bend Radius (Installation)    | $\leq 20 \times \text{Overall Cable Diameter}$                                                                          |
| 19                                                                                                     | Minimum Bend Radius (Installed)       | $\leq 10 \times \text{Overall Cable Diameter}$                                                                          |
| 20                                                                                                     | Minimum Tensile Strength (Short Term) | $\geq 1600 \text{ N}$                                                                                                   |
| 21                                                                                                     | Minimum Crush Resistance              | $\geq 3000 \text{ N} / 100 \text{ mm}$                                                                                  |
| 22                                                                                                     | Operating Temperature                 | $-20^{\circ}\text{C}$ to $+70^{\circ}\text{C}$ or better                                                                |
| 23                                                                                                     | Installation Suitability              | Suitable for outdoor ducts, underground installation, direct burial and campus backbone applications                    |
| 24                                                                                                     | Splicing Compatibility                | Suitable for fusion splicing                                                                                            |
| 25                                                                                                     | Identification                        | Sequential metre marking on outer sheath                                                                                |
| 26                                                                                                     | Compliance                            | Factory tested and compliant with applicable IEC/ITU standards                                                          |

|    |            |                                                                                                    |
|----|------------|----------------------------------------------------------------------------------------------------|
| 27 | Compliance | The offered Optical Fiber Cable shall be part of the OEM's end-to-end structured cabling solution. |
| 28 | Warranty   | minimum 25-year OEM Application Warranty,                                                          |

| <b>Fiber Optic Rack Mount LIU (Loaded)-Various Fiber Counts</b> |                          |                                                                                                                                                                           |
|-----------------------------------------------------------------|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Approved/Eligible OEMs : CommScope/Molex/Legrand</b>         |                          |                                                                                                                                                                           |
| <b>Sr. No.</b>                                                  | <b>Parameter</b>         | <b>Minimum Technical Specification</b>                                                                                                                                    |
| 1                                                               | Product                  | Rack Mount Fiber Optic LIU (Fully Loaded) with adapters, pigtails, splice trays and splice protection accessories corresponding to the port capacity specified in the BOQ |
| 2                                                               | Application              | Termination, splicing, protection and management of Single Mode Optical Fiber Cables                                                                                      |
| 3                                                               | Mounting                 | 19-inch Rack Mount, suitable for standard network racks                                                                                                                   |
| 4                                                               | Rack Height              | 1U or suitable rack height as per offered port density                                                                                                                    |
| 5                                                               | Fiber Type               | Single Mode OS2 (9/125 $\mu$ m)                                                                                                                                           |
| 6                                                               | Number of Ports          | As specified in the BOQ                                                                                                                                                   |
| 7                                                               | Connector Type           | LC Duplex Adapter                                                                                                                                                         |
| 8                                                               | Adapter Colour           | Blue (for Single Mode) or OEM Standard                                                                                                                                    |
| 9                                                               | Adapter Compliance       | IEC 61754, IEC 61300 or equivalent                                                                                                                                        |
| 10                                                              | Pigtails                 | Factory-terminated Single Mode OS2 LC Pigtails, fully loaded                                                                                                              |
| 11                                                              | Pigtail Fibre Standard   | ITU-T G.652.D, backward compatible with G.657.A1 or higher                                                                                                                |
| 12                                                              | Ferrule                  | Ceramic Zirconia Ferrule                                                                                                                                                  |
| 13                                                              | Insertion Loss (Adapter) | $\leq 0.30$ dB (Typical), $\leq 0.50$ dB (Maximum)                                                                                                                        |
| 14                                                              | Return Loss              | $\geq 50$ dB (UPC) or $\geq 60$ dB (APC, if applicable)                                                                                                                   |
| 15                                                              | Mating Durability        | Minimum 500 mating cycles                                                                                                                                                 |
| 16                                                              | Splice Tray              | Modular splice tray with splice protectors for all terminated fibres                                                                                                      |
| 17                                                              | Cable Management         | Front cable management with fibre routing, bend-radius protection and cable strain relief                                                                                 |
| 18                                                              | Access                   | Hinged, sliding or removable access mechanism for easy installation and maintenance                                                                                       |
| 19                                                              | Fibre Protection         | Integrated fibre management with bend-radius control and fibre routing guides                                                                                             |
| 20                                                              | Material                 | CRCA Steel / Aluminium or equivalent with powder-coated finish                                                                                                            |
| 21                                                              | Finish                   | Powder Coated, corrosion-resistant                                                                                                                                        |
| 22                                                              | Operating Temperature    | -20°C to +70°C or better                                                                                                                                                  |
| 23                                                              | Standards                | IEC 61753, IEC 61754, IEC 61300, ISO/IEC 11801, RoHS Compliant                                                                                                            |
| 24                                                              | Accessories              | Complete with adapters, pigtails, splice trays, splice protectors, cable glands, mounting hardware, labels and all accessories required for complete installation         |
| 25                                                              | Warranty                 | minimum 25-year OEM Application Warranty,                                                                                                                                 |

| <b>LC-LC Duplex Single Mode Optical Fiber Patch Cord (3 m / 10 m)</b> |                       |                                                                                                                                        |
|-----------------------------------------------------------------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Approved/Eligible OEMs : CommScope/Molex/Legrand</b>               |                       |                                                                                                                                        |
| <b>Sr. No.</b>                                                        | <b>Parameter</b>      | <b>Minimum Technical Specification</b>                                                                                                 |
| 1                                                                     | Product               | LC-LC Duplex Single Mode Optical Fiber Patch Cord                                                                                      |
| 2                                                                     | Application           | Interconnection between LIU, Optical Transceivers and Network Equipment                                                                |
| 3                                                                     | Fiber Type            | Single Mode OS2 (9/125 µm)                                                                                                             |
| 4                                                                     | Fiber Standard        | ITU-T G.652.D, bend-insensitive ITU-T G.657.A1 or higher                                                                               |
| 5                                                                     | Cable Construction    | Duplex Zip Cord                                                                                                                        |
| 6                                                                     | Length                | As specified in the BOQ                                                                                                                |
| 7                                                                     | Connector Type        | LC Duplex to LC Duplex                                                                                                                 |
| 8                                                                     | Connector Polish      | UPC (unless otherwise specified in the BOQ)                                                                                            |
| 9                                                                     | Connector Ferrule     | Ceramic Zirconia                                                                                                                       |
| 10                                                                    | Insertion Loss        | ≤ 0.30 dB (Typical), ≤ 0.50 dB (Maximum) per connector                                                                                 |
| 11                                                                    | Return Loss           | ≥ 50 dB (UPC)                                                                                                                          |
| 12                                                                    | Jacket Material       | LSZH (Low Smoke Zero Halogen)                                                                                                          |
| 13                                                                    | Jacket Colour         | Yellow or OEM Standard for Single Mode                                                                                                 |
| 14                                                                    | Cord Construction     | OEM Standard suitable for enterprise structured cabling                                                                                |
| 15                                                                    | Tensile Member        | OEM Standard                                                                                                                           |
| 16                                                                    | Operating Temperature | -20°C to +70°C or better                                                                                                               |
| 17                                                                    | Standards             | IEC 61753, IEC 61754, IEC 61300, ISO/IEC 11801, RoHS Compliant                                                                         |
| 18                                                                    | Compatibility         | Compatible with the offered LIU, optical fibre cable and transceivers. The patch cords shall be factory terminated and factory tested. |
| 19                                                                    | Warranty              | minimum 25-year OEM Application Warranty,                                                                                              |

| <b>Category 6A UTP Indoor Cable</b>                     |                  |                                        |
|---------------------------------------------------------|------------------|----------------------------------------|
| <b>Approved/Eligible OEMs : CommScope/Molex/Legrand</b> |                  |                                        |
| <b>Sr. No.</b>                                          | <b>Parameter</b> | <b>Minimum Technical Specification</b> |
| 1                                                       | Product          | Category 6A UTP Cable (Indoor)         |
| 2                                                       | Cable Type       | 4 Pair UTP                             |
| 3                                                       | Conductor        | 23 AWG Solid Bare Copper               |
| 4                                                       | Insulation       | Polyethylene (PE) or OEM Standard      |
| 5                                                       | Separator        | Cross Separator or OEM Standard        |
| 6                                                       | Jacket Material  | LSZH / FRLSZH                          |
| 7                                                       | Jacket Colour    | OEM Standard                           |

|    |               |                                                     |
|----|---------------|-----------------------------------------------------|
| 8  | Performance   | ANSI/TIA Category 6A, ISO/IEC Class EA              |
| 9  | Bandwidth     | Minimum 500 MHz                                     |
| 10 | Data Rate     | 10GBASE-T up to 100 metres                          |
| 11 | PoE Support   | IEEE 802.3af/at/bt (PoE++)                          |
| 12 | Standards     | ANSI/TIA-568.2-D, ISO/IEC 11801, IEC 61156, RoHS    |
| 13 | Cable Length  | Standard OEM Box/Reel Length                        |
| 14 | Warranty      | minimum 25-year OEM Application Warranty,           |
| 15 | Compatibility | All passive components shall be mutually compatible |

| Category 6A Outdoor Cable                        |                     |                                                     |
|--------------------------------------------------|---------------------|-----------------------------------------------------|
| Approved/Eligible OEMs : CommScope/Molex/Legrand |                     |                                                     |
| Sr. No.                                          | Parameter           | Minimum Technical Specification                     |
| 1                                                | Product             | Category 6A Outdoor UTP Cable                       |
| 2                                                | Cable Type          | 4 Pair UTP                                          |
| 3                                                | Conductor           | 23 AWG Solid Bare Copper                            |
| 4                                                | Jacket Material     | UV Stabilized HDPE / PE                             |
| 5                                                | UV Protection       | Required                                            |
| 6                                                | Moisture Resistance | Required                                            |
| 7                                                | Performance         | ANSI/TIA Category 6A                                |
| 8                                                | Bandwidth           | Minimum 500 MHz                                     |
| 9                                                | Data Rate           | 10GBASE-T up to 100 metres                          |
| 10                                               | PoE Support         | IEEE 802.3bt PoE++                                  |
| 11                                               | Standards           | ANSI/TIA-568.2-D, ISO/IEC 11801, IEC 61156, RoHS    |
| 12                                               | Installation        | Outdoor conduit, tray or exposed installation       |
| 13                                               | Warranty            | minimum 25-year OEM Application Warranty,           |
| 14                                               | Compatibility       | All passive components shall be mutually compatible |

| Category 6A Keystone Jack                        |                  |                                                     |
|--------------------------------------------------|------------------|-----------------------------------------------------|
| Approved/Eligible OEMs : CommScope/Molex/Legrand |                  |                                                     |
| Sr. No.                                          | Parameter        | Minimum Technical Specification                     |
| 1                                                | Product          | Category 6A Keystone Jack                           |
| 2                                                | Type             | Tool-less or 110 IDC Termination                    |
| 3                                                | Compatibility    | Standard Modular Faceplate & Patch Panel            |
| 4                                                | Performance      | ANSI/TIA Category 6A                                |
| 5                                                | Connector        | RJ45                                                |
| 6                                                | Contact Material | Phosphor Bronze with Gold Plating                   |
| 7                                                | IDC              | 110 Type                                            |
| 8                                                | Standards        | ANSI/TIA-568.2-D, ISO/IEC 11801                     |
| 9                                                | PoE Support      | IEEE 802.3bt                                        |
| 10                                               | Warranty         | minimum 25-year OEM Application Warranty,           |
| 11                                               | Compatibility    | All passive components shall be mutually compatible |

| Faceplate                                        |               |                                                     |
|--------------------------------------------------|---------------|-----------------------------------------------------|
| Approved/Eligible OEMs : CommScope/Molex/Legrand |               |                                                     |
| Sr. No.                                          | Parameter     | Minimum Technical Specification                     |
| 1                                                | Product       | Single Port Faceplate                               |
| 2                                                | Material      | High Impact Flame Retardant Plastic                 |
| 3                                                | Colour        | White or OEM Standard                               |
| 4                                                | Mounting      | Flush Mount                                         |
| 5                                                | Compatibility | Standard Modular Keystone Jack                      |
| 6                                                | Label Window  | Required                                            |
| 7                                                | Standards     | RoHS                                                |
| 8                                                | Warranty      | minimum 25-year OEM Application Warranty,           |
| 9                                                | Compatibility | All passive components shall be mutually compatible |

| Category 6A Loaded Patch Panel                   |                  |                                                     |
|--------------------------------------------------|------------------|-----------------------------------------------------|
| Approved/Eligible OEMs : CommScope/Molex/Legrand |                  |                                                     |
| Sr. No.                                          | Parameter        | Minimum Technical Specification                     |
| 1                                                | Product          | Category 6A Loaded Patch Panel                      |
| 2                                                | Mounting         | 19-inch Rack Mount                                  |
| 3                                                | Ports            | As specified in BOQ                                 |
| 4                                                | Height           | 1U or OEM Standard                                  |
| 5                                                | Jack Type        | Category 6A RJ45                                    |
| 6                                                | Cable Management | Rear Cable Manager                                  |
| 7                                                | Labelling        | Port Identification                                 |
| 8                                                | Performance      | ANSI/TIA Category 6A                                |
| 9                                                | Standards        | ANSI/TIA-568.2-D, ISO/IEC 11801                     |
| 10                                               | Warranty         | minimum 25-year OEM Application Warranty,           |
| 11                                               | Compatibility    | All passive components shall be mutually compatible |

| Category 6A Patch Cord                           |             |                                 |
|--------------------------------------------------|-------------|---------------------------------|
| Approved/Eligible OEMs : CommScope/Molex/Legrand |             |                                 |
| Sr. No.                                          | Parameter   | Minimum Technical Specification |
| 1                                                | Product     | Category 6A Patch Cord          |
| 2                                                | Length      | As specified in BOQ             |
| 3                                                | Conductor   | Stranded Copper                 |
| 4                                                | Connector   | RJ45-RJ45                       |
| 5                                                | Boot        | Snagless                        |
| 6                                                | Jacket      | LSZH                            |
| 7                                                | Performance | Category 6A                     |
| 8                                                | Bandwidth   | 500 MHz                         |

|    |               |                                                     |
|----|---------------|-----------------------------------------------------|
| 9  | PoE Support   | IEEE 802.3bt                                        |
| 10 | Standards     | ANSI/TIA-568.2-D, ISO/IEC 11801                     |
| 11 | Warranty      | minimum 25-year OEM Application Warranty,           |
| 12 | Compatibility | All passive components shall be mutually compatible |

| <b>RJ45 Connector (Indoor)</b>                          |                  |                                                     |
|---------------------------------------------------------|------------------|-----------------------------------------------------|
| <b>Approved/Eligible OEMs : CommScope/Molex/Legrand</b> |                  |                                                     |
| <b>Sr. No.</b>                                          | <b>Parameter</b> | <b>Minimum Technical Specification</b>              |
| 1                                                       | Product          | RJ45 Plug for Category 6A                           |
| 2                                                       | Compatibility    | Category 6A Cable                                   |
| 3                                                       | Contact          | Gold Plated                                         |
| 4                                                       | Housing          | Polycarbonate                                       |
| 5                                                       | Performance      | Category 6A                                         |
| 6                                                       | Standards        | IEC 60603-7, ANSI/TIA-568.2-D                       |
| 7                                                       | Warranty         | minimum 25-year OEM Application Warranty,           |
| 8                                                       | Compatibility    | All passive components shall be mutually compatible |

| <b>Industrial RJ45 Connector (Outdoor Wi-Fi)</b>        |                       |                                                     |
|---------------------------------------------------------|-----------------------|-----------------------------------------------------|
| <b>Approved/Eligible OEMs : CommScope/Molex/Legrand</b> |                       |                                                     |
| <b>Sr. No.</b>                                          | <b>Parameter</b>      | <b>Minimum Technical Specification</b>              |
| 1                                                       | Product               | Industrial / Outdoor RJ45 Connector                 |
| 2                                                       | Compatibility         | Category 6A Outdoor Cable                           |
| 3                                                       | Protection            | IP67 or better (when mated)                         |
| 4                                                       | Housing               | Metal                                               |
| 5                                                       | Connector Type        | Shielded RJ45                                       |
| 6                                                       | Environmental         | Dustproof & Waterproof                              |
| 7                                                       | Operating Temperature | -20°C to +70°C or better                            |
| 8                                                       | Standards             | IEC 60603-7, RoHS                                   |
| 9                                                       | Warranty              | minimum 25-year OEM Application Warranty,           |
| 10                                                      | Compatibility         | All passive components shall be mutually compatible |

| <b>Floor Standing Network Rack (12U / 24U / 42U)</b>    |                  |                                                                                                                                                                                                |
|---------------------------------------------------------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Approved/Eligible OEMs : CommScope/Molex/Legrand</b> |                  |                                                                                                                                                                                                |
| <b>Sr. No.</b>                                          | <b>Parameter</b> | <b>Minimum Technical Specification</b>                                                                                                                                                         |
| 1                                                       | Product          | Floor Standing Network Rack Complete with cage nuts, bolts, cable managers, blanking panels (where required), shelves (if required), fan tray, PDU, earthing kit and all mounting accessories. |
| 2                                                       | Rack Height      | As specified in the BOQ                                                                                                                                                                        |
| 3                                                       | Standard         | 19-inch Equipment Mounting                                                                                                                                                                     |
| 4                                                       | Rack Width       | 600 mm or 800 mm (OEM Standard / as required)                                                                                                                                                  |

|    |                               |                                                                                                        |
|----|-------------------------------|--------------------------------------------------------------------------------------------------------|
| 5  | Rack Depth                    | Suitable for the proposed equipment (minimum 800 mm for active equipment or as per OEM recommendation) |
| 6  | Construction                  | Welded / Modular CRCA Steel Construction                                                               |
| 7  | Material Thickness            | Minimum 1.6 mm (Mounting Rails), Minimum 1.2 mm (Other Members) or OEM Standard                        |
| 8  | Front Door                    | Lockable Toughened Glass / Perforated Metal Door                                                       |
| 9  | Rear Door                     | Lockable Steel/Perforated Door                                                                         |
| 10 | Side Panels                   | Lockable & Removable                                                                                   |
| 11 | Mounting Rails                | Adjustable Front & Rear                                                                                |
| 12 | Static Load Capacity          | Minimum 500 kg or suitable for the offered equipment                                                   |
| 13 | Dynamic Load Capacity         | Minimum 300 kg                                                                                         |
| 14 | Cable Entry                   | Top and Bottom                                                                                         |
| 15 | Cable Management              | Vertical & Horizontal Cable Managers                                                                   |
| 16 | Ventilation                   | Fan Mounting Provision with Ventilation Slots                                                          |
| 17 | Cooling Fans                  | Minimum 2 Fans or as required                                                                          |
| 18 | Power Distribution Unit (PDU) | Minimum 6/8 Socket Horizontal PDU with MCB or as specified                                             |
| 19 | Earthing                      | Dedicated Earthing Stud                                                                                |
| 20 | Finish                        | Powder Coated                                                                                          |
| 21 | Colour                        | OEM Standard (Black/Grey)                                                                              |
| 22 | Compliance                    | EIA-310-D, IEC 60297, RoHS                                                                             |
| 23 | Compatibility                 | Compatible with all offered active and passive network equipment.                                      |
| 24 | Cable Management              | Proper segregation of copper, fibre and power cables with bend-radius protection.                      |
| 25 | Warranty                      | Minimum 5-year OEM warranty                                                                            |

| <b>Wall Mount Rack (9U)</b>     |                  |                                                                                                                                                                                            |
|---------------------------------|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Approved/Eligible OEMs :</b> |                  |                                                                                                                                                                                            |
| <b>Sr. No.</b>                  | <b>Parameter</b> | <b>Minimum Technical Specification</b>                                                                                                                                                     |
| 1                               | Product          | Wall Mount Network Rack Complete with cage nuts, bolts, cable managers, blanking panels (where required), shelves (if required), fan tray, PDU, earthing kit and all mounting accessories. |
| 2                               | Rack Height      | As specified in the BOQ                                                                                                                                                                    |
| 3                               | Rack Depth       | Suitable for the proposed equipment (minimum 800 mm for active equipment or as per OEM recommendation)                                                                                     |
| 4                               | Standard         | 19-inch Rack                                                                                                                                                                               |
| 5                               | Construction     | CRCA Steel                                                                                                                                                                                 |
| 6                               | Front Door       | Lockable Toughened Glass                                                                                                                                                                   |
| 7                               | Side Panels      | Removable                                                                                                                                                                                  |
| 8                               | Mounting Rails   | Adjustable                                                                                                                                                                                 |
| 9                               | Cable Entry      | Top & Bottom                                                                                                                                                                               |

|    |                  |                                                                                   |
|----|------------------|-----------------------------------------------------------------------------------|
| 10 | Ventilation      | Ventilation Slots with Fan Mount Provision                                        |
| 11 | Load Capacity    | Minimum 60 kg                                                                     |
| 12 | Finish           | Powder Coated                                                                     |
| 13 | Earthing         | Earthing Stud                                                                     |
| 14 | Compliance       | EIA-310-D / IEC 60297                                                             |
| 15 | Compatibility    | Compatible with all offered active and passive network equipment.                 |
| 16 | Cable Management | Proper segregation of copper, fibre and power cables with bend-radius protection. |
| 17 | Warranty         | Minimum 5-year OEM warranty                                                       |

| Outdoor IP65 Network Rack |                       |                                                                                                                                                                                                      |
|---------------------------|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Approved/Eligible OEMs :  |                       |                                                                                                                                                                                                      |
| Sr. No.                   | Parameter             | Minimum Technical Specification                                                                                                                                                                      |
| 1                         | Product               | Outdoor Weatherproof Network Rack Complete with cage nuts, bolts, cable managers, blanking panels (where required), shelves (if required), fan tray, PDU, earthing kit and all mounting accessories. |
| 2                         | Rack Height           | As specified in the BOQ                                                                                                                                                                              |
| 3                         | Rack Depth            | Suitable for the proposed equipment (minimum 800 mm for active equipment or as per OEM recommendation)                                                                                               |
| 4                         | Standard              | 19-inch Rack                                                                                                                                                                                         |
| 5                         | Protection            | Minimum IP65                                                                                                                                                                                         |
| 6                         | Material              | CRCA Steel / Galvanized Steel / Aluminium (OEM Standard)                                                                                                                                             |
| 7                         | Coating               | Outdoor Powder Coating with Corrosion Resistance                                                                                                                                                     |
| 8                         | Door                  | Lockable Front Door with Weatherproof Gasket                                                                                                                                                         |
| 9                         | Cooling               | Fan with Thermostat and Ventilation Arrangement or Heat Exchanger (as applicable)                                                                                                                    |
| 10                        | Cable Entry           | Weatherproof Cable Glands                                                                                                                                                                            |
| 11                        | PDU                   | Suitable Power Distribution Unit                                                                                                                                                                     |
| 12                        | Earthing              | Internal and External Earthing Provision                                                                                                                                                             |
| 13                        | Mounting              | Wall / Pole / Floor Mount (as applicable)                                                                                                                                                            |
| 14                        | Operating Temperature | -10°C to +55°C or better                                                                                                                                                                             |
| 15                        | Compliance            | IP65, IEC 60529, RoHS                                                                                                                                                                                |

|    |                      |                                                                                                                                                                                                           |
|----|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 16 | General Requirement  | Suitable for outdoor installation under all weather conditions and Protection against dust, rain, humidity and UV exposure.                                                                               |
| 17 | Compatibility        | Compatible with all offered active and passive network equipment.                                                                                                                                         |
| 18 | Cable Management     | Proper segregation of copper, fibre and power cables with bend-radius protection.                                                                                                                         |
| 19 | Warranty             | Minimum 7-year OEM warranty                                                                                                                                                                               |
| 20 | Outdoor Rack Cooling | OEM must provide an appropriate thermal management solution (fan with thermostat, filtered ventilation, or heat exchanger, depending on the equipment's heat dissipation) to maintain reliable operation. |

| Approved/Eligible OEMs : |                 |                                                               |
|--------------------------|-----------------|---------------------------------------------------------------|
| Sr. No.                  | Parameter       | Minimum Technical Specification                               |
| 1                        | Product         | HDPE Pipe                                                     |
| 2                        | Size            | 25 mm OD                                                      |
| 3                        | Material        | High Density Polyethylene (HDPE)                              |
| 4                        | Type            | Telecom Grade Duct                                            |
| 5                        | Pressure Rating | Minimum PN 6 or suitable for underground telecom applications |
| 6                        | Colour          | Black with coloured identification stripes or OEM Standard    |
| 7                        | UV Resistance   | Required                                                      |
| 8                        | Installation    | Suitable for underground cable laying                         |
| 9                        | Standard        | IS 4984 / TEC / BIS applicable standards                      |

| Approved/Eligible OEMs : |               |                                 |
|--------------------------|---------------|---------------------------------|
| Sr. No.                  | Parameter     | Minimum Technical Specification |
| 1                        | Product       | PVC Back Box                    |
| 2                        | Type          | Square                          |
| 3                        | Material      | High Impact Flame Retardant PVC |
| 4                        | Compatibility | Suitable for modular faceplate  |
| 5                        | Mounting      | Flush / Surface Mount           |
| 6                        | Colour        | White                           |
| 7                        | Standard      | ISI/BIS                         |

| <b>Reinforced Flexible Pipe (32 mm)</b> |                  |                                         |
|-----------------------------------------|------------------|-----------------------------------------|
| <b>Approved/Eligible OEMs :</b>         |                  |                                         |
| <b>Sr. No.</b>                          | <b>Parameter</b> | <b>Minimum Technical Specification</b>  |
| 1                                       | Product          | Reinforced Flexible Conduit             |
| 2                                       | Size             | 32 mm                                   |
| 3                                       | Material         | Heavy Duty PVC Reinforced Flexible Pipe |
| 4                                       | Application      | Indoor/Outdoor Cable Protection         |
| 5                                       | Flexibility      | High                                    |
| 6                                       | UV Resistance    | Required (for outdoor installation)     |
| 7                                       | Standard         | BIS applicable standards                |

| <b>MS Clamp for Access Point Mounting</b> |                  |                                         |
|-------------------------------------------|------------------|-----------------------------------------|
| <b>Approved/Eligible OEMs :</b>           |                  |                                         |
| <b>Sr. No.</b>                            | <b>Parameter</b> | <b>Minimum Technical Specification</b>  |
| 1                                         | Product          | Mild Steel Mounting Clamp               |
| 2                                         | Material         | Galvanized Mild Steel                   |
| 3                                         | Thickness        | Minimum 2 mm                            |
| 4                                         | Finish           | Hot Dip Galvanized / Powder Coated      |
| 5                                         | Mounting         | Wall/Ceiling/Pole Compatible            |
| 6                                         | Load Capacity    | Suitable for offered Wi-Fi Access Point |
| 7                                         | Accessories      | SS Fasteners, Nuts, Bolts, Washers      |

| <b>PVC Conduit with Accessories</b> |                  |                                                                   |
|-------------------------------------|------------------|-------------------------------------------------------------------|
| <b>Approved/Eligible OEMs :</b>     |                  |                                                                   |
| <b>Sr. No.</b>                      | <b>Parameter</b> | <b>Minimum Technical Specification</b>                            |
| 1                                   | Product          | PVC Conduit                                                       |
| 2                                   | Size             | 25 mm                                                             |
| 3                                   | Material         | Heavy Duty Rigid PVC                                              |
| 4                                   | Type             | ISI Marked                                                        |
| 5                                   | Colour           | White / Grey                                                      |
| 6                                   | Accessories      | Couplers, Bends, Junction Boxes, Saddles, End Caps, Adhesive etc. |
| 7                                   | Standard         | IS 9537                                                           |

| <b>PVC Flexible Pipe</b>        |                  |                                        |
|---------------------------------|------------------|----------------------------------------|
| <b>Approved/Eligible OEMs :</b> |                  |                                        |
| <b>Sr. No.</b>                  | <b>Parameter</b> | <b>Minimum Technical Specification</b> |
| 1                               | Product          | PVC Flexible Conduit                   |
| 2                               | Size             | 32 mm                                  |
| 3                               | Material         | Flexible PVC                           |

|   |          |                          |
|---|----------|--------------------------|
| 4 | Type     | Heavy Duty               |
| 5 | Colour   | Grey / Black             |
| 6 | Standard | BIS applicable standards |

| Standard Pole (3 Metre)  |                    |                                                              |
|--------------------------|--------------------|--------------------------------------------------------------|
| Approved/Eligible OEMs : |                    |                                                              |
| Sr. No.                  | Parameter          | Minimum Technical Specification                              |
| 1                        | Product            | Pole for Wi-Fi Access Point Mounting                         |
| 2                        | Height             | 3 Metres                                                     |
| 3                        | Material           | Hot Dip Galvanized Mild Steel (GI/MS)                        |
| 4                        | Wall Thickness     | Minimum 3 mm                                                 |
| 5                        | Finish             | Hot Dip Galvanized                                           |
| 6                        | Mounting           | Base Plate with Foundation Bolts                             |
| 7                        | Wind Resistance    | Suitable for outdoor installation                            |
| 8                        | Earthing Provision | Required                                                     |
| 9                        | Accessories        | Foundation Bolts, Cable Entry Arrangement, Mounting Brackets |

Note:

- a. All conduits, ducts, pipes, clamps, brackets, poles, back boxes, mounting accessories, fasteners, anchors, supports, and other civil/electrical accessories shall be of heavy-duty construction, corrosion-resistant where applicable, suitable for the intended installation environment, and conform to the relevant BIS/ISI or equivalent standards.
- b. The bidder shall supply all incidental materials required for complete installation, even if not individually listed in the BOQ, without any additional cost to the Purchaser.

## Buyback of Existing IT & Wi-Fi Infrastructure

The Successful Bidder shall undertake the buyback of the existing IT and Wi-Fi infrastructure identified by the Tenderer as part of this project. The buyback shall be done only after successful completion of the first event. The buyback shall include collection, dismantling, transportation, handling and lawful disposal/recycling or refurbishment of the identified equipment in accordance with the applicable statutory provisions.

The buyback shall include, but not be limited to, the following activities:

- a. Dismantling of the identified existing active and passive network equipment without causing damage to the surrounding infrastructure.
- b. Collection and transportation of the identified equipment from the designated locations.
- c. Submission of an inventory acknowledging receipt of the equipment duly signed by the authorised representatives of the Successful Bidder and the Tenderer.

d. Compliance with all applicable environmental, e-Waste Management Rules, Government of India guidelines, and other statutory requirements for handling and disposal of electronic equipment.

e. Any expenses towards dismantling, packing, loading, transportation, insurance, labour, recycling, disposal or refurbishment shall be borne by the Successful Bidder and shall be deemed included in the quoted prices.

f. The Successful Bidder shall ensure that no Government data or configuration remains on any storage media before removal of the equipment. Wherever applicable, secure data sanitization shall be carried out in the presence of the Tenderer before removal of the equipment.

g. The Successful Bidder shall issue an Equipment Handover Receipt and, wherever applicable, a Certificate of Recycling/Disposal from an authorised recycler.

## Commercial Clause

The bidder shall quote the **buyback value** for the existing infrastructure separately in the prescribed BOQ. The quoted buyback value shall be deducted from the total project cost for the purpose of financial evaluation and payment, as specified in the BOQ.

## As-Is Condition

The existing equipment proposed for buyback shall be offered on an **"As Is Where Is", "As Is What Is", and "No Complaint" basis**. The Tenderer does not guarantee the functionality, condition, completeness or residual value of any equipment offered under the buyback scheme.

## Ownership

Ownership of the existing equipment identified under the buyback shall be transferred to the Successful Bidder only after successful Go-Live of the project

### **Tentative List of buyback items:**

| <b>Sr. No.</b> | <b>Equipment Type</b>     | <b>Make</b> | <b>Model</b>     | <b>Qty</b> |
|----------------|---------------------------|-------------|------------------|------------|
| 1              | Cisco Wireless Controller | Cisco       | Cisco 5520       | 1          |
| 2              | Cisco Switch              | Cisco       | WS-C3850-16XS-S  | 2          |
| 3              | Cisco Switch              | Cisco       | WS-2960X         | 4          |
| 4              | Cisco Switch              | Cisco       | SG300-28MP-K9-EU | 12         |
| 5              | Cisco Access Points       | Cisco       | AIR-AP1562I-D-K9 | 33         |
| 6              | Cisco Access Points       | Cisco       | AIR-AP1852I-D-K9 | 10         |
| 7              | Cisco Access Points       | Cisco       | AIR-AP2802I-D-K9 | 94         |
| 8              | DLINK Switch              | DLINK       |                  | 4          |
| 9              | Firewall                  | Netgear     |                  | 1          |

# Annexure A

## Format of Earnest Money Deposit in the form of Bank Guarantee

Ref:

Bank Guarantee No.

Date:

To,

GM (Networking)

Gujarat Informatics Ltd,

Block No. 2, 2nd Floor, C & D Wing, Karmayogi Bhavan

Sector - 10 A, Gandhinagar – 382010.

Whereas ----- (here in after called "the Bidder") has submitted its bid dated ----- in response to the Tender no: \_\_\_\_\_ KNOW ALL MEN by these presents that WE -----  
--- having our registered office at ----- (hereinafter called "the Bank") are bound unto the Gujarat Informatics Limited in the sum of ----- for which payment well and truly to be made to Gujarat Informatics Limited , the Bank binds itself, its successors and assigns by these presents. Sealed with the Common Seal of the said Bank this -----day of -----2026.

### THE CONDITIONS of this obligation are:

#### 1. The E.M.D. may be forfeited:

- a. if a Bidder withdraws its bid during the period of bid validity
- b. Does not accept the correction of errors made in the tender document;
- c. In case of a successful Bidder, if the Bidder fails:
  - (i) To sign the Contract as mentioned above within the time limit stipulated by purchaser  
or
  - (ii) To furnish performance bank guarantee as mentioned above or
  - (iii) If the bidder is found to be involved in fraudulent practices.
  - (iv) If the bidder fails to submit the copy of purchase order & acceptance thereof.
  - (v) "If the successful bidder fails to submit the Performance Bank Guarantee & sign the Contract Form within prescribed time limit, the EMD of the successful bidder will be forfeited. Tenderer also reserves the right to blacklist such bidder from participating in future tenders if sufficient cause exists.

We undertake to pay to the GIL/Purchaser up to the above amount upon receipt of its first written demand, without GIL/ Purchaser having to substantiate its demand, provided that in its demand GIL/ Purchaser will specify that the amount claimed by it is due to it owing to the occurrence of any of the abovementioned conditions, specifying the occurred condition or conditions.

This guarantee will remain valid up to the validity of Bid +90 days. The Bank undertakes not to revoke this guarantee during its currency without previous consent of the OWNER/PURCHASER and further agrees that if this guarantee is extended for a period as mutually agreed between bidder & owner/purchaser, the guarantee shall be valid for a period so extended provided that a written request for such extension is received before the expiry of validity of guarantee.

The Bank shall not be released of its obligations under these presents by any exercise by the OWNER/PURCHASER of its liability with reference to the matters aforesaid or any of them or by reason or any other acts of omission or commission on the part of the OWNER/PURCHASER or any other indulgence shown by the OWNER/PURCHASER or by any other matter or things.

The Bank also agree that the OWNER/PURCHASER at its option shall be entitled to enforce this Guarantee against the Bank as a Principal Debtor, in the first instance without proceeding against the SELLER and notwithstanding any security or other guarantee that the OWNER/PURCHASER may have in relation to the SELLER's liabilities.

Dated at \_\_\_\_\_ on this \_\_\_\_\_ day of \_\_\_\_\_ 2026.

\_\_\_\_\_

Signed and delivered by

\_\_\_\_\_

For & on Behalf of

Name of the Bank & Branch &

Its official Address

**Approved Bank:** Banks (operating in India having branch at Ahmedabad/ Gandhinagar) as per the Finance Department latest GR or further instruction issued by Finance department time to time.

## Performance Bank Guarantee

(To be stamped in accordance with Stamp Act)

Ref:

Bank Guarantee No.

Date:

To

Name & Address of the Purchaser/Indenter

\_\_\_\_\_  
  
\_\_\_\_\_

Dear Sir,

In consideration of Name & Address of the Purchaser/Indenter, Government of Gujarat, Gandhinagar (hereinafter referred to as the OWNER/PURCHASER which expression shall unless repugnant to the context or meaning thereof include successors, administrators and assigns) having awarded to M/s. \_\_\_\_\_ having Principal Office at \_\_\_\_\_ (hereinafter referred to as the "SELLER" which expression shall unless repugnant to the context or meaning thereof include their respective successors, administrators, executors and assigns) the supply of \_\_\_\_\_ by issue of Purchase Order No. \_\_\_\_\_ Dated \_\_\_\_\_ issued by Gujarat Informatics Ltd., Gandhinagar for and on behalf of the OWNER/PURCHASER and the same having been accepted by the SELLER resulting into CONTRACT for supplies of materials/equipments as mentioned in the said purchase order and the SELLER having agreed to provide a Contract Performance and Warranty Guarantee for faithful performance of the aforementioned contract and warranty quality to the OWNER/PURCHASER, \_\_\_\_\_ having Head Office at (hereinafter referred to as the 'Bank' which expressly shall, unless repugnant to the context or meaning thereof include successors, administrators, executors and assigns) do hereby guarantee to undertake to pay the sum of Rs. \_\_\_\_\_ (Rupees \_\_\_\_\_) to the OWNER/PURCHASER on demand at any time up to \_\_\_\_\_ without a reference to the SELLER. Any such demand made by the OWNER/PURCHASER on the Bank shall be conclusive and binding notwithstanding any difference between Tribunals, Arbitrator or any other authority.

The Bank undertakes not to revoke this guarantee during its currency without previous consent of the OWNER/PURCHASER and further agrees that the guarantee herein contained shall continue to be enforceable till the OWNER/PURCHASER discharges this guarantee. OWNER/PURCHASER shall have the fullest liberty without affecting in any way the liability of the Bank under this guarantee from time to time to extend the time for performance by the SELLER of the aforementioned CONTRACT. The OWNER/ PURCHASER shall have the fullest liberty, without affecting this guarantee, to postpone from time to time the exercise of any powers vested in them or of any right which they might have against the SELLER, and to exercise the same at any time in any manner, and either to enforce to forebear to enforce any covenants contained or implied, in the aforementioned CONTRACT between the OWNER/PURCHASER and the SELLER or any other course of or remedy or security available to the OWNER/PURCHASER.

The Bank shall not be released of its obligations under these presents by any exercise by the OWNER/PURCHASER of its liability with reference to the matters aforesaid or any of them or by reason or any other acts of omission or commission on the part of the OWNER/PURCHASER or any other indulgence shown by the OWNER/PURCHASER or by any other matter or things.

The Bank also agree that the OWNER/PURCHASER at its option shall be entitled to enforce this Guarantee against the Bank as a Principal Debtor, in the first instance without proceeding against the SELLER and not withstanding any security or other guarantee that the OWNER/PURCHASER may have in relation to the SELLER's liabilities.

Notwithstanding anything contained herein above our liability under this Guarantee is restricted to Rs. \_\_\_\_\_ (Rupees \_\_\_\_\_) and it shall remain in force up to and including \_\_\_\_\_ and shall be extended from time to time for such period as may be desired by the SELLER on whose behalf this guarantee has been given.

Dated at \_\_\_\_\_ on this \_\_\_\_\_ day of \_\_\_\_\_ 2026.

\_\_\_\_\_  
Signed and delivered by

\_\_\_\_\_  
For & on Behalf of

Name of the Bank & Branch &

Its official Address

List of approved Banks

Banks (operating in India having branch at Ahmedabad/ Gandhinagar) as per the Finance Department latest GR or further instruction issued by Finance department time to time.

Bidders are requested to kindly go through the Office Memorandum No.: F. No.6/18/2019-PPD dated 23.07.2020 & Office Memorandum No.: F.18/37/2020-PPD dated 08.02.2021 of Ministry of Finance, Dept. of Expenditure, Public Procurement division related restrictions on procurement from border countries. As per this GR, bidders are required to quote/offer the product which adheres to this GR. The undertaking as from bidder as well as from offered product OEM is required to be submitted along with bid as per given Performa.

## On letterhead of Bidder

**Sub: Undertaking as per Office Memorandum No.: F. No.6/18/2019-PPD dated 23.07.2020 & Office Memorandum No.: F.18/37/2020-PPD dated 08.02.2021 of Ministry of Finance, Dept. of Expenditure, Public Procurement division**

Ref: Bid Number: \_\_\_\_\_

I have read the clause regarding restriction on procurement from a bidder of a country which shares a land border with India. I certify that we as a bidder and quoted product from following OEMs are not from such a country or, if from such a country, these quoted products OEM has been registered with competent authority. I hereby certify that these quoted product & its OEM fulfils all requirements in this regard and is eligible to be considered for procurement for Bid number: \_\_\_\_\_

| No. | Item Category | Quoted Make & Model |
|-----|---------------|---------------------|
| 1   |               |                     |
| 2   |               |                     |

In case I'm supplying material from a country which shares a land border with India, I will provide evidence for valid registration by the competent authority, otherwise GIL/End user Dept. reserves the right to take legal action on us.

(Signature)

Authorized Signatory of **M/s <<Name of Company>>**

# On letterhead of OEM

**Sub: Undertaking as per Office Memorandum No.: F. No.6/18/2019-PPD dated 23.07.2020 & Office Memorandum No.: F.18/37/2020-PPD dated 08.02.2021 of Ministry of Finance, Dept. of Expenditure, Public Procurement division**

**Ref: Bid Number:** \_\_\_\_\_

Dear Sir,

I have read the clause regarding restriction on procurement from a bidder of a country which shares a land border with India. I certify that our quoted product and our company are not from such a country, or if from such a country, our quoted product and our company have been registered with competent authority. I hereby certify that these quoted product and our company fulfils all requirements in this regard and is eligible to be considered for procurement for Bid number: \_\_\_\_\_

| No. | Item Category | Quoted Make & Model |
|-----|---------------|---------------------|
|     |               |                     |
|     |               |                     |

In case I'm supplying material from a country which shares a land border with India, I will provide evidence for valid registration by the competent authority; otherwise GIL/End user Dept. reserves the right to take legal action on us.

(Signature)

Authorized Signatory of **M/s <<Name of Company>>**

# Performa of Compliance letter/Authenticity of Information Provided

(On Non judicial Stamp paper of Rs. 300 duly attested by the First class Magistrate/Notary Public)

Date:

To,

**GM (Networking)**

**Gujarat Informatics Ltd,**

**Block No. 2, 2<sup>nd</sup> Floor, C & D Wing, Karmayogi Bhavan**

**Sector - 10 A, Gandhinagar – 382010.**

**Sub: Compliance with the tender terms and conditions, specifications and Eligibility Criteria**

Ref: Tender no. \_\_\_\_\_

Dear Sir,

With reference to above referred tender, I, undersigned <<Name of Signatory>>, in the capacity of <<Designation of Signatory>>, is authorized to give the undertaking on behalf of <<Name of the bidder>>.

We wish to inform you that we have read and understood the technical specification and total requirement of the above mentioned bid submitted by us.

We hereby confirm that all our quoted items meet or exceed the requirement and are absolutely compliant with specifications mentioned in the bid document.

We also explicitly understand that all quoted items meet technical specification of the bid & that such technical specification overrides the brochures/standard literature if the same contradicts or is absent in brochures.

In case of breach of any tender terms and conditions or deviation from bid specification other than already specified as mentioned above, the decision of Tender Committee for disqualification will be accepted by us.

The Information provided in our submitted bid is correct. In case any information provided by us are found to be false or incorrect, you have right to reject our bid at any stage including forfeiture of our EMD/ PBG/cancel the award of contract. In this event, tenderer reserves the right to take legal action on us.

Thanking you,

Dated this \_\_\_\_\_ day of \_\_\_\_\_ 2026

Signature: \_\_\_\_\_

(in the Capacity of) : \_\_\_\_\_

Duly authorized to sign bid for and on behalf of

\_\_\_\_\_

**Note: This form should be signed by authorized signatory of bidder**