



Bharatiya Vidya Bhavan's
Sardar Patel College of Engineering
(Govt. Aided Autonomous Institute Affiliated to University of Mumbai)
Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai 400058.



Request for Proposal for IEEE 802.11-Based Campus-Wide Wireless LAN System

1. Sealed proposals are invited for an **IEEE 802.11-Based Campus-Wide Wireless LAN System** for the Institute premises.
2. The vendors need to submit the most competitive bid for the items as per the RFP documents enclosed.
3. The quantities of each item in the BoQ, along with the unit prices in INR and the applicable taxes, should be indicated clearly in the proposal.
4. The submitted proposal shall remain valid for 15 days after the last date of submission.
5. The purchaser will conduct a technical evaluation and a commercial evaluation to compare the received proposals and determine the substantially responsive bidder before placing the PO.
6. Payment will be released within one week after a satisfactory installation and completion report from the technical team of the Institute.
7. The institute reserves the right to withdraw this RFP without assigning any reason.
8. A detailed RFP document is enclosed with this notice.
9. The proposals should be submitted in two parts: (a) Technical bid and (b) Commercial bid in separate sealed envelopes. The envelope containing both the bids should be submitted in one envelope to the **Institute Stores, Room No. 48, Ground Floor, on or before 20.03.2026 upto 5.00 pm.**

Date: 11.03.2026

Encl: As above




I/c. Principal
Bharatiya Vidya Bhavan's
Sardar Patel College of Engineering
Government Aided Autonomous Institute
Munshi Nagar, Andheri (West), Mumbai - 58



Bharatiya Vidya Bhavan's
Sardar Patel College of Engineering
(Govt. Aided Autonomous Institute Affiliated to University of Mumbai)
Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai 400058.



Request for Proposal for IEEE 802.11-Based Campus-Wide Wireless LAN System

Sardar Patel College of Engineering (SPCE) intends to upgrade and expand its campus wireless network to provide reliable, high-speed, and secure Wi-Fi connectivity for students, faculty, staff, and guests within the SPCE Main Building. The proposed solution should support high-density academic environments, seamless mobility, and secure access to institutional resources while ensuring optimal performance and scalability for future growth.

The selected bidder shall design, supply, install, configure, test, and commission the required wireless LAN solution in accordance with the technical specifications mentioned in this RFQ. The solution should provide robust coverage, high performance, centralised management, and strong security features suitable for a modern campus environment.

Refer to the following sections for technical specifications, QoS, coverage and performance requirements, scope of work, licenses, qualification and eligibility criteria for bidders, terms of the SLA, warranty conditions, and other relevant details.

A) Technical Specifications

For Indoor access points	
Sr. No.	Technical Specifications
1	The access point radio should support a minimum 2x2 MIMO with 2 special streams on 2.4 GHz and a minimum 2x4 MIMO with 4 special streams on 5 GHz.
2	An access point should have a Dual Radio 802.11ax access point with OFDMA and Multi-User MIMO (MU-MIMO)
3	Access point should support 802.11ax Target Wait Time (TWT) to support low-power client devices.
4	Access point should support BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, and 1024 QAM modulation types
5	Minimum aggregate data rate of 3 Gbps.
6	The access point should be 802.11ax-ready from day one and support WPA2, WPA3 (Enterprise & Personal), and Enhanced Open security from day one. Also support RADIUS & Active Directory integration, MAC authentication, 802.1x authentication, or Captive portal authentication.
7	The access point should support Transmit beam-forming (TxBF) to improve signal reliability and range.
8	Access point should support 802.11ax Target Wait Time (TWT) to support low-power client devices.
9	The Access Point should support advanced wireless security features, including secure guest network access with at least 16 SSIDs, captive portal authentication (e.g., SMS-based login or equivalent), and rogue access point detection, to ensure safe and reliable wireless network access for both guest and internal users.
10	The wireless system should support Rogue AP detection, Wireless Intrusion Detection System (WIDS), and Wireless Intrusion Prevention System (WIPS).
11	The WLAN solution must support automatic channel selection, transmit power control, band steering, and load balancing to optimize wireless performance in high-density environments.
12	APs must support 802.11k, 802.11v, and 802.11r standards for fast, seamless layer-2 roaming in high-density campus deployments.
13	An access point should support at least 16 SSIDs/BSSIDs per radio.

14	The management platform should support automatic RF optimisation, including channel and transmit power adjustment.
15	AP should have one multi-gigabit Ethernet port (RJ-45, maximum negotiated speed 2.5Gbps) or One standard Gigabit (1Gbps) LAN port
16	The Access Point should support IEEE 802.3af/at PoE power input through the Ethernet port, with optional DC power adapter support.
17	The access point should also include an option for an external power adapter.
18	An access point should have a Console/management port, preferably.
19	An access point can have an integrated internal antenna.
20	The maximum transmit power of the AP and antenna should comply with WPC norms for indoor access points. OEM to give an undertaking letter stating that the AP will be configured as per WPC guidelines for indoor AP, and also submit the WPC certificate showing approval.
21	The wireless solution must support centralised management via a hardware controller or a virtual controller architecture, without requiring a license-based hardware change. The proposed access points must support zero-touch provisioning (ZTP) for automatic onboarding and configuration. A centralised management dashboard must be provided for monitoring, configuration, firmware upgrades, and performance analytics of all deployed access points.
22	Minimum 200 active concurrent users per AP.
23	AP shall support management access via the Web GUI (HTTPS/SSL), the Mobile App (Android/iOS), SSH, and SNMPv3.
24	Access point must comply with Indian WPC regulations for indoor deployment, FCC/CE, and UL 2043 (plenum rating)
25	The access point must be Wi-Fi Alliance-certified (Wi-Fi 6).
26	Access point must support Maximum Ratio Combining (MRC), Space-Time Block Coding (STBC), and Low Density Parity Check (LDPC). The equipment must comply with WPC India regulations, and the OEM must provide a valid WPC/ETA approval certificate for the quoted model.
27	The Indoor access point shall be supplied with a standard mounting kit suitable for wall and ceiling installation. The mounting bracket shall support False ceiling (T-grid) mounting, Solid ceiling mounting, and Wall mounting.
28	All wireless LAN network components, such as APs, controllers, transceivers, and (SX, LX, LR) modules, should be from the same OEM.
29	The additional items, such as network switches, suggested for the successful implementation of the wireless LAN solution and to meet the configuration's operational requirements, should preferably be from the same OEM or compatible with the access points and other accessories.
30	The network management software should preferably be from the same OEM or from a third party.
31	If the network switches and network management software are not from the same OEM as the access points, then seamless connectivity, control, and performance at the time of installation and during the warranty period are within the scope of the bidder and the OEM.

Outdoor Access Points	
Sr. No.	Technical Specifications
1	The access point radio should support a minimum 2x2 MIMO with 2 special streams on 2.4 GHz and a minimum 4x4 MIMO with 4 special streams on 5 GHz.
2	An access point should be a Dual-Radio 802.11ax access point with OFDMA and Multi-User MIMO (MU-MIMO).
3	The access point should support 802.11ax Target Wait Time (TWT) to support low-power client devices.
4	The access point should support BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, and 1024-QAM modulation types.

5	Minimum aggregate data rate of 3 Gbps.
6	The access point should be 802.11ax-ready from day one and support WPA2, WPA3 (Enterprise & Personal), and Enhanced Open security from day one. Also, support RADIUS & Active Directory integration, MAC authentication, 802.1x authentication, or Captive portal authentication.
7	The access point should support Transmit beam-forming (TxBF) to improve signal reliability and range.
8	Access point should support 802.11ax Target Wait Time (TWT) to support low-power client devices.
9	The Access Point should support advanced wireless security features, including secure guest network access with at least 16 SSIDs, captive portal authentication (e.g., SMS-based login or equivalent), and rogue access point detection, to ensure safe and reliable wireless network access for both guest and internal users.
10	The WLAN solution must support automatic channel selection, transmit power control, band steering, and load balancing to optimize wireless performance in high-density environments.
11	APs must support 802.11k, 802.11v, and 802.11r standards for fast, seamless layer-2 roaming in high-density campus deployments.
12	Access point shall support intelligent client association control to improve roaming efficiency and prevent client devices from remaining connected to suboptimal access points.
13	An access point should support at least 16 SSIDs/BSSIDs per radio.
14	The management platform should support automatic RF optimisation, including channel and transmit power adjustment.
15	AP should have one multi-gigabit Ethernet port (RJ-45, maximum negotiated speed 2.5Gbps) or One standard Gigabit (1Gbps) LAN port
16	The access point should support the 802.3af/at PoE standard (Outdoor PoE-compliant). Grounding provision must be available.
17	The wireless system should support Rogue AP detection, Wireless Intrusion Detection System (WIDS), and Wireless Intrusion Prevention System (WIPS).
18	The access point should also include an option for an external power adapter.
19	An access point should preferably have a Console/management port.
20	Outdoor-rated integrated antennas preferred.
21	Access point must support maximum Ratio Combining (MRC), Space-Time Block Coding (STBC), and Low Density Parity Check (LDPC). Transmit power must comply with WPC India regulations for outdoor deployment. OEM must provide the WPC approval certificate and undertaking.
22	Minimum IP67-rated enclosure (dust-tight and water immersion protection). Operating temperature range: minimum -20°C to +55°C (or better).
23	Minimum 200 active concurrent users per AP
24	The access point must be designed for outdoor deployment and must support wind resistance suitable for pole mounting. The device must include surge protection for the Ethernet port and ESD protection. The enclosure must be UV-resistant for long-term outdoor exposure. The access point must be supplied with a pole-mounting kit and a wall-mounting kit (where applicable). All mounting accessories and hardware must be corrosion-resistant and suitable for outdoor installation.
25	The wireless solution must support centralised management via a hardware controller or a virtual controller architecture, without requiring a license-based hardware change. The proposed access points must support zero-touch provisioning (ZTP) for automatic onboarding and configuration. A centralised management dashboard must be provided for monitoring, configuration, firmware upgrades, and performance analytics of all deployed access points.
26	AP shall support management access via the Web GUI (HTTPS/SSL), the Mobile App (Android/iOS), SSH, and SNMPv3.
27	Access point must comply with WPC India (Outdoor approval), FCC / CE, UL 2043 (plenum rating)
28	The access point must be Wi-Fi Alliance-certified (Wi-Fi 6).
29	Access point should be UL outdoor safety standards certified.

30	All wireless LAN network components, such as APs, controllers, transceivers, and (SX, LX, LR) modules, should be from the same OEM.
31	The additional items, such as network switches, suggested for the successful implementation of the wireless LAN solution and to meet the configuration's operational requirements, should preferably be from the same OEM or compatible with the access points and other accessories.
32	The network management software should preferably be from the same OEM or from a third party.
33	If the network switches and the network management software are not from the same OEM as the access points, then seamless connectivity control and performance at the time of installation and during the warranty period are within the scope of the bidder and the OEM.

A) Quality of Service (QoS) Requirements

1. The WLAN solution must support Wi-Fi Multimedia (WMM) for prioritization of Voice, Video, Best Effort, and Background traffic categories.
2. Self-healing (on detection of RF interference or loss of RF coverage).
3. Dynamic load balancing to automatically distribute clients to the least loaded 802.11 channel and AP
4. Support fast roaming feature.
5. Support band steering where 5 GHz clients are preferred to connect over 5GHz Radio to provide better load balancing among 2.4GHz and 5GHz Radios
6. The solution must support dynamic QoS policy enforcement integrated with authentication mechanisms (e.g., 802.1X/RADIUS).
7. The solution should provide support capabilities to raise critical alarms by sending an email, an SMS, or an SNMP message to the IT team.
8. The system must support SSID-based and user-based bandwidth control and rate limiting.
9. Supports smarter roaming and client load balancing on both IPv4 and IPv6 networks.

Inline Security Features

1. Secure Guest Portal: Solution should support local web-based authentication; access (hotspot URL redirection for user login); and provisioning: customisation of login/welcome pages. This portal should facilitate a simple process for creating short-lived guest IDs and automatically expiring passwords. Support for creating logins for attendees of short events, such as conferences, should also be provided.
2. AP should allow authenticated client devices to roam securely from one access point to another AP within or across subnets. There should not be any perceptible delay during re-association.
3. Support for classifying different types of Rogue AP detection and protection
4. Support wireless IPS functionality.
5. Support IP filtering policies or ACLs
6. Support Radius, LDAP, and Single Sign-On (SSO) integration
7. The solution should provide options for profiling devices and mapping specific VLANs
8. The solution should detect DOS attacks and wireless intrusions and terminate rogue access points.

B) Wireless Intrusion Detection & Prevention (WIDS/WIPS)

1. The Access Point must support a built-in Wireless Intrusion Detection System (WIDS) for continuous monitoring of the RF spectrum.
2. The solution must support a Wireless Intrusion Prevention System (WIPS) capable of automatically detecting and containing rogue access points and unauthorised wireless clients.
3. The system must detect and classify:
 - Rogue APs (internal and external)
 - Evil twin access points
 - Unauthorised/ad-hoc networks
 - MAC spoofing attempts
 - De-authentication and disassociation attacks

4. The solution must provide automatic containment of rogue APs without requiring additional dedicated security sensors.
5. WIDS/WIPS functionality must operate in real-time and generate alerts through the centralised management platform.
6. The WLAN solution must support dedicated or dynamic scanning radios for continuous security monitoring without affecting client performance.
7. The system must maintain event logs and security reports and support export to Syslog/SIEM platforms.
8. WIDS/WIPS capabilities must be native to the OEM WLAN solution and must not require third-party security appliances.

C) Coverage & Performance Requirement

1. The Institute will provide the floor plan of the area to be covered under the proposed Wi-Fi solution. The Access Point placement layout shall be prepared and submitted by the bidder based on the site survey. The bidder shall conduct a comprehensive RF site survey and provide heat maps, coverage design, capacity planning, and bill of materials as part of the technical proposal.
2. The bidder shall design, supply, install, configure, and commission a wireless network solution that ensures seamless, high-performance Wi-Fi coverage for the area under consideration, as shown in the floor plan provided by the Institute (i.e., across the entire SPCE Main Building, including all indoor and required outdoor areas).
3. The bidder shall be solely responsible for determining the number and placement of Access Points to cover the entire area under consideration, as per the floor plan provided, with the minimum signal strength tabulated below.
4. No separate payment shall be made for additional Access Points required to achieve compliance with this section.

Minimum Signal Strength Requirement

1. Minimum RSSI ≥ -65 dBm in all usable indoor areas.
2. Minimum RSSI ≥ -65 dBm in all usable indoor areas.
3. Signal-to-Noise Ratio (SNR) ≥ 25 dB.
4. No dead zones in academic and administrative areas.
5. Coverage shall be validated through a post-installation active RF site survey.

High-Density Performance Requirement

The wireless network shall be designed to support high-density usage scenarios, including classrooms, laboratories, and library areas. The solution must ensure:

1. Stable connectivity under concurrent user load.
2. Seamless roaming without session drops.
3. Consistent throughput during peak academic hours.
4. No noticeable service degradation in high-occupancy areas.

Seamless Mobility Requirement

The solution shall support seamless Layer 2 and Layer 3 roaming compliant with 802.11k, 802.11v, and 802.11r standards. Users moving between floors or departments shall not experience:

1. Session drops
2. Re-authentication delays
3. Noticeable performance degradation

D) Scope of the Work

1. The bidder shall supply, transport to the site, provide transit insurance, install, configure, and demonstrate all the specified features of the proposed wireless solution.
2. The bidder shall provide all the documentation, including Architecture, Design, Deployment diagrams, test plans, operating and service manuals, diagrams, and test reports of the deployed WLAN system, both in hard and electronic copy versions."
3. The Access Point placement layout, as per the Institute's floor plan, shall be prepared and submitted by the bidder based on the site survey. The bidder shall conduct a comprehensive RF site survey and provide heat maps, coverage design, capacity planning, and bill of materials as part of the technical proposal.
4. Bidders should provide all documents/manuals useful for daily administration.
5. The bidder shall bear all costs during the preparation and submission of the proposal, site visit (if required), etc.
6. The Institute has the right to cancel the PO if the delivery, installation, and acceptance testing are not completed within the stipulated timeline. Specifically
 - Delivery should be within 8-10 weeks of the PO issuance.
 - Installation, commissioning, and acceptance testing should be completed within 10-12 weeks of delivery.
7. The warranty period is counted from the date the installation is completed, and the acceptance certificate is issued by SPCE.
8. The installation will be performed by certified, trained engineers from Bidder/OEM for wireless controllers, followed by well-documented, comprehensive user training.
9. OEM will provide an undertaking that OEM is responsible for a 5-year performance guarantee and 2-year AMC period.
10. Any hardware or software item not specifically mentioned in the technical specifications but required for the successful implementation of the wireless LAN solution and for meeting the operational requirements of the configuration must be listed and quoted separately in the bid.
11. The cost of such items will be considered for commercial evaluation along with the costs of the access points and other supporting accessories.
12. The entire installation should be carried out only at the proposed site. Requests for remote access for installation/fine-tuning will not be entertained during the installation period.
13. The successful bidder may be required to configure the scheduling mechanism of the proposed solution so that the existing LAN in the current SPCE Network facility is not disturbed.
14. Bidders should quote for the products and models specified in the technical specification table, with the service level agreement as mentioned elsewhere in the document.
15. If the specific model is not available, the bidder can quote a product with higher specifications, capabilities, and compatibility. Bidders cannot quote for products with inferior specifications.
16. Laying CAT6 cable (material and labour charges) from existing network switches to the proposed access point locations is within the vendor's scope. The CAT6 cable used should be of the Comm
17. -Scope brand.
18. The vendor may quote cable-laying charges (material + labour) per meter and also indicate the total cost for the entire length of the cable-laying.
19. End-to-end termination, switch installation and configuration, patch panel installation, numbering patch cords (panel side), end-to-end numbering, testing, cable pulling, conduit pipe fitting, flexible pipe fitting, HDPE pipe installation, labelling & documentation, fluke testing of CAT6, etc.

E) Licenses

Controller Type	On-Premises Controller-Based Solution
AP License	All AP adoption licenses included.
Subscription	No mandatory recurring subscription shall be required for the core WLAN functionality of all Access Points and network switches. The Access Points must continue to operate and broadcast SSIDs even after the expiry of support or subscription licenses. Basic WLAN features such as SSID broadcasting, client connectivity, and local management must remain functional without any mandatory license renewal.
License Validity	The proposed solution, along with Access points, must be supported by the OEM/Bidder for a minimum of 7 Years (5-year warranty and 2-year AMC).
Firmware & Updates	5 years of firmware, security patches, and upgrades included
Feature Availability	WPA3, 802.1X, VLAN, Roaming features included without an extra license
Cloud Dependency	Core WLAN must function without cloud connectivity.
Hidden Cost	No hidden license or add-on charges
Post-License Operation	APs must continue broadcasting after support expiry.
License Disclosure	A detailed license BOM must be submitted.
Support	The Partner must have a dedicated support team with remote and on-site support availability at the SPCE Campus.
Pre-deployment Documentation	Partner consultants must provide Proposed Design and Architecture presentations that include best-practice approaches. The partner consultant must provide a Heat Map.
Post-deployment Documentation	The partner team must provide the SPCE team with a detailed implementation document and training.
Post-deployment survey	Partner must provide the Post-deployment site survey report with the vendor diagnostic tool for sign-off

F) Qualification Criteria For Bidder And OEM

1. The OEM for Access Points and allied active network components must appear in the latest Gartner Magic Quadrant for Enterprise Wired and Wireless LAN Infrastructure for at least 3 consecutive years. Documentary proof from the official Gartner publication must be submitted along with the bid.
2. OEM must be in the core business of Wireless network solutions and must have a presence in India for a minimum of 3 years.
3. The bidder should be an authorised representative of the OEM. The bidder shall furnish the manufacturer's authorisation (MAF) letter from the respective OEMs, specific to this tender, mentioning the tender number for which the authorisation is being provided.
4. OEM must provide on-site hardware replacement and technical support services on the same day or the Next Business Day (NBD) from OEM-authorized engineers. Support delivery through a partner-only service model will not be accepted. Same-day support response and NBD replacement commitment must be backed by OEM support documentation.
5. The bidder should be an OEM-certified wireless solution supplier and integrator.
6. Bidders should have an adequately documented track record of supplying and installing Wi-Fi access points (at least 500 access points supplied over the last 5 years).
7. The bidder/OEM should have local support in Maharashtra.
8. The Technical Assistance Centre (TAC) and R&D should be based in India.
9. The bidder should have valid documentary proof of the GST registration number. It is mandatory to enclose all the supporting documents.

H) Service Level Agreement - Warranty & Support

1. Provide support and maintenance services for the Wireless Access Points to ensure optimal performance.
2. Replace faulty or non-functioning Wireless Access Points at no additional cost to SPCE.
3. OEM must provide direct Next Business Day (NBD) onsite hardware replacement and technical support services from OEM-authorized engineers. Support delivery through a partner-only service model will not be accepted. Same-day support response and NBD replacement commitment must be backed by OEM support documentation.
4. During the warranty period, the OEM/bidder will have to undertake comprehensive maintenance of all hardware components, equipment, and software support supplied by the vendor at the equipment's installation location (every 6 months).
5. The proposed Access Points and allied active network components shall have a minimum 5-year comprehensive warranty, including advance hardware replacement. The warranty must also include firmware updates, security patches, and software upgrades for the entire warranty period without additional cost.
6. Technical support for system administration/maintenance of the WLAN solution should be provided throughout the warranty period.
7. The time duration for the complete rollout of the proposed solution is up to 18 weeks from the date of the formal purchase order.
8. Documentation to be provided (After installation)
 - RF survey for proposed locations of the Institute.
 - Step-by-step installation and configuration guide for the WLAN solution from start.
 - Wireless Controller Configuration and Integration
 - Basic troubleshooting for wireless users and access points
 - Basic troubleshooting for wireless controllers
 - Health status check of wireless controllers and access points.
 - Any other document/manual useful for daily administration.
9. The bidder should submit a copy of the service agreement contract to SPCE within 3 months of the contract award.

ANNEXURE I - Performance Statement Proforma (for a period of the last three years)

Name of the Company :

Order Placed by (full name and address of the purchaser)	Order number and date	Description and quality of the ordered equipment	Value of order	Date of completion of delivery as per contract	Remarks indicating reasons for late delivery, if any, and justification for the price difference of their supply order	Has the equipment been installed properly? (submit a certificate from the purchaser)	Contact details

Signature and Seal of the Manufacturer / Bidder

Place:

Date:

ANNEXURE II - Bidder's Information

Name of the Bidder	
Address of the Bidder	
PAN No.	
GSTIN No.	
State of GST Registration	
Email ID	
Contact Person's Name & Designation	
Mobile No.	

ANNEXURE III – QUESTIONNAIRE

Sr. No.	Questions	Response
1	Whether all the terms and conditions of the SPCE document have been complied with. Compliance (Yes/No)	
2	Whether all the items specified in the technical specification have been compiled and quoted in the bidding engine. Compliance (Yes/No)	
3	Confirm that you have read all the instructions carefully and have complied with the instructions accordingly. Compliance (Yes/No)	
4	In case the bidder does not manufacture goods, they have submitted the Manufacturer's Authorisation letter. Compliance (Yes/No)	
5	Mention the Delivery period.	
6	Mention the Warranty of the material.	
7	Mention the HSN/SAC code of the material.	
8	Mention the nearest International Airport/nearest Port of shipment (in case of FOB/FCA).	

ANNEXURE IV – MANUFACTURING AUTHORIZATION FORM

Date:

Ref No.:

To,
The Principal
SPCE, Mumbai

Subject: Manufacturer Authorisation for Supply of Wireless LAN Solution

Dear Sir/Madam,

We, [Name of Manufacturer / OEM], having our registered office at [OEM Address], do hereby authorise [Name of Bidder / Partner Company], having its registered office at [Bidder Address], to quote, supply, install, configure, and provide support for our Wireless LAN products against your RFQ No. [Reference Number] for the project titled: "Supply, Installation & Commissioning of Wi-Fi Solution for SPCE Main Building."

We hereby confirm that:

1. The products quoted by the bidder are genuine, new, and sourced directly from us.
2. We authorise the bidder to participate in the above-mentioned tender for our products.
3. We shall provide full technical support, firmware updates, and warranty support for a minimum period of 5 years as specified in the tender.
4. The products supplied shall comply with all technical specifications mentioned in the RFQ.
5. We confirm the availability of spare parts and technical support in India.
6. If the authorised bidder fails to fulfil its warranty obligations, we shall provide the necessary support directly or through our authorised service channels.

This authorisation is valid only for the above-mentioned tender.

For [OEM Name]

Authorized Signatory

Name:

Designation:

Email:

Contact Number:

Company Seal & Signature