Board of Management, Quaid-E-Azam Industrial Estate,
Kot Lakhpat, Lahore

Bidding Document

Board of Management
Quaid -e-Azam Industrial Estate

"PROCUREMENT, INSTALLATION, COMMISSIONING OF WIRELESS NETWORK IN QIE BUILDING"

at

BOARD OF MANAGEMENT QUAID-E-AZAM INDUSTRIAL ESTATE

BOARD OF MANAGEMENT ★ Quaid-e-Azam Industrial Estate ★
1
Sr. Estate Manager

Int

BIDDING DOCUMENT

"PROCUREMENT, INSTALLATION, COMMISSIONING OF WIRELESS NETWORK IN QIE BUILDING"

at

Board of Management, Quaid-E-Azam Industrial Estate, Kot Lakhpat, Lahore

Last date of submission: 04-12-2024 (up to 03:15 pm)

Init.

INVITATION TO e-BID

Board of Management Quaid-e-Azam Industrial Estate (BOM QIE) invites electronic bids from the original manufacturers / authorized distributors / suppliers / contractors / service providers etc. registered with Income Tax and Sales Tax Department for the Procurement, Supply, Installation, Testing and commissioning of Networking System in QIE.

e-biddingdocuments as per regulations, contained detailed terms and conditions, specifications and requirement etc. are available for the registered bidders on PPRA website: www.ppra.punjab.gov.pk, BOM QIE website www.qie.com.pk and EPADS Portal i.e. http://punjab.eprocure.gov.pk free of cost.

General Terms & Conditions:

- As per Punjab Procurement Rules-2014. Rule 38(1) single stage two envelope bidding procedure will be applicable.
- Bid must contain Bid Security in shape of CDR / Pay Order amounting to Rs. 45,677/- against the project estimated cost Rs.2,283,809/- in favor of "PIEDMC Quaid-e-Azam Industrial Estate Board Lahore" (which is 2% of the estimated cost) without which the offer shall be rejected being non-responsive. The bid security must be attached in readable PDF format and submitted in original in Undersigned office address.
- Technical and Financial Separate bids, duly completed, signed, stamp an in complete conformity with Tender Documents must be submitted online E-Pak Acquisition and Disposal System (EPADS) Portal i.e. http://punjab.eprocure.gov.pk till 04-12-2024 by or before 03:15 PM and bids shall be opened on same date at 03:45 PM, as per the PPRA Rules, 2014.
- Bids that are incomplete, not signed and stamped, late or submitted by other than specified mode will not be considered.
- For bids submission on E-Procurement, Bidders are requested to register at www.punjab.eprocure.gov.pk.
- All rates must be inclusive of all applicable govt. taxes. Any bidder not fulfilling the eligibility criteria given in bidding documents will be considered ineligible for bidding.

Tariq Hussain

Sr. Estate Manager,
Board of Management
169-A/S, Quaid-e-Azam Industrial Estate
(Kot Lakhpat) Lahore
Phone No. 042-99330357-9

1. Overview

Board of Management, Quaid-E-Azam Industrial Estate, Kot Lakhpat, Lahore intends "Procurement, Installation, Commissioning of Wireless Network in QIE Building as provided at **Annex 'A'** and technical scope of work at **Annex 'B'**. The supplier will be responsible for Supply , Installation and Commissioning of items, wherever required, at the Board of Management, Quaid-E-Azam Industrial Estate, Kot Lakhpat, Lahore. This document provides complete instructions for bidders intending to participate in this Bidding.

2. Instructions for Bidders

2 . 1 Purchase will be made as per PPRA Rules 2014, as amended to date single stage two envelopes procedure PPRA Rule. The Board of Management, Quaid-E-Azam Industrial Estate, Kot Lakhpat, Lahore invites bids from manufacturers, suppliers and distributors for supplyas per specifications given in the Bidding Documents.

2 . 2 The bids shall be submitted on E-PAD (mandatory). Proposals submitted/ processed on EPAD will be accepted otherwise bid will be rejected. The complete E-bids must be submitted online on e-procurement system (E-pads) website i.e. www.punjab.eprocure.gov.pk Bidders are advised to ensure uploading the Bids on EPADS portal, well before the submission of deadline.

2.3 Response to the Tender (Bid) should be submitted/uploaded on EPADS which shall include two separated bids of Technical **Proposal and** Financial **Proposal** before **03:15 PM** on **04-12-2024.** Technical Proposals will be opened on same day at **03:45 PM** and Financial Proposals will be opened after completion of technical evaluation. The exact time for opening of financial proposals will be informed to technically qualified bidders and opening time date will also be updated on EPADS.

Sr. Estate Manager,
169-A/S, Quaid-e-Azam Industrial Estate, (Kot Lakhpat), Lahore
Ph: +92 42 99330357-9
Email: info@qie.com.pk , Website: www.qie.com.pk

2.4 All bids must be submitted/ uploaded by filling the Annex 'C'. Same should be enclosed in the financial proposal. Bidder must use the same numbers and labels used in this

BOARD OF MANAGEMENT ★ Quaid-e-Azam Industrial Estate ★
Sr. Estate Manager

Int.

Request for Proposal.

2.5 The original Bidding Document duly signed and officially sealed by the bidder must be submitted / uploaded complete in all respect with the proposals. Any conditional, ambiguous, incomplete, supplementary or revised offer after the opening of Tender shall not be entertained.

3. Technical Proposal Format

Bidders are required to include the following documents/information in their technical proposals in the order given below:

i. Profile of company complete in all respect.

ii. List of Previous and Current customers, Purchase Orders should be attached with technical bid.

iii. Legal registered entity (Sole Proprietor, Registration with SECP or Registrar of Firm) having valid NTN, GST and PST if applicable

iv. Complete Income Tax Returns for Last three fiscal Years

v. An affidavit on Rs 100/- Stamp Paper issued after date of publishing of Tender Notice/Invitation to Bid which illustrate that currently they are not black listed or de-barred by any Government/Semi- Government Department/ Autonomous body to participate in bidding. Failure to submit such affidavit may lead to disqualification.

vi. Details of all the items & specifications provided by supplier against items detailed as given at **Annex 'A'**

vii. Acceptance of technical scope of work as provided in **Annex 'B'**

viii. Proposed delivery schedule for delivery of items.

ix. Signed and Stamped Complete bidding document.

x. Bank Draft of the Bid Security attached with technical proposal estimated cost mentioned in the Tender notice/Invitation to Bid.

xi. Minimum 1 to 3 years' experience (Firm must attach five related supply orders as a proof with the technical bid)

4. Financial Proposal Format

Financial Proposal must include the following in the order given below:

i. Prices duly entered on the form in the attached BOQ

ii. Validity period of the quoted price

BOARD OF MANAGEMENT
Quaid-e-Azam Industrial Estate
Sr. Estate Manager

5. Terms & Conditions

5.1 This invitation for bids is open to all national original Manufacturers/ Distributors/Suppliers in Pakistan.

5.2 All prices should be quoted in Pak Rupees and inclusive of all Government Taxes & Levies.

5.3 A bank draft equal to 2% of the total estimated cost mentioned in Tender notice/Invitation to e-Bid should accompany the Bidding Document as **Bid Security** drawn in favor of **PIEDMC-Quaid-e-Azam Industrial Estate Board, Lahore**. The Bidding Document shall not be considered without Bid Security. Bank draft for Bid Security must be attached on EPADS under Bid security details and also attached with technical Bid in PDF Form and original Bid Security must be submitted in with Company's request letter in QIE Office situated at 169-A/S, Board of Management Quaid-e-Azam Industrial Estate (Kot Lakhpat) Lahore before deadline.

5.4 Bid Security for bidders not selected will be returned a minimum of two weeks after announcement of award and returned to successful bidder after issuance of Purchase order/work order. If the selected bidder fails to accept the work order/purchase order with in stipulated time, Bid Security will be forfeited.

5.5 A Bank draft of 10% of the total amount as **Performance Guarantee** will be provided by the supplier in favor of **PIEDMC-Quaid-e-Azam Industrial Estate Board, Lahore** after issuance of Purchase Order/Work Order which shall remain valid for 12 months beyond delivery period. This performance guarantee will be released after the completion of warranty/guarantee period.

5.6 The decision of the QIE competent authority will be binding on all concerned and will in no case be challenged in any forum.

5.7 Board of Management, Quaid-E-Azam Industrial Estate, Kot Lakhpat, Lahore reserves the right to modify the conditions / specificationsof the Bidding Document with intimation to all the participants who have downloaded the Bidding Document from EPADS, PPRA and QIE Website.

5.8 Delivery period will be as per terms & conditions of purchase order/work order.

5.9 Delivery shall be completed according to the agreed upon schedule as per terms & conditions of purchase order/supply order.

5.10 In case the selected bidder fails to execute the work order/purchase order strictly in accordance with the terms and conditions laid down in the purchase order/work order,

BOARD OF MANAGEMENT ★ Quaid-e-Azam Industrial Estate ★
Sr. Estate Manager

the Performance Guarantee shall be forfeited.

5.11 The Board of Management, Quaid-E-Azam Industrial Estate, Kot Lakhpat, Lahore will get all the items inspected at BOM, QIE Office situated at 169-A/S, Board of Management Quaid-e-Azam Industrial Estate (Kot Lakhpat) Lahore and reject the Item, if not found according to the stated specifications.

5.12 The Board of Management, Quaid-E-Azam Industrial Estate, Kot Lakhpat, Lahore reserves the right to claim compensation for the losses caused by delay in the delivery of items.

5.13 It is the sole responsibility of the bidder to comply with local, national and international laws.

5.14 In case any supplies is found not in conformity with the specifications provided in the Bidding document, either on account of inferior quality, defective workmanship, faulty design, or is short supplied, or wrongly supplied, the supplier will replace the same free of chargesor pay the full cost of replacement.

5.15 All the proposals submitted online through EPADS will become the property of the Board of Management, Quaid-E-Azam Industrial Estate, Kot Lakhpat, Lahore.

5.16 All prices should be valid for 180 days. Withdrawal or any modification of the original offer within the validity period shall entitle the Board of Management, Quaid-E-Azam Industrial Estate, Kot Lakhpat, Lahore to forfeit the Bid Security in favor of the Board of Management, Quaid-E-Azam Industrial Estate, Kot Lakhpat, Lahore and/or putting a ban on the future inquires or taking any other suitable action against the bidder.

5.17 Delivery of all the Items will be free of charge at BOM, QIE Office situated at 169-A/S, Board of Management Quaid-e-Azam Industrial Estate (Kot Lakhpat) Lahore during the office hours with a copy of Delivery Challan.

5.18 All Items should be brand-new and according to order specification and covered under normal warranty/guarantee etc. as mentioned in the quote.

6 Evaluation Criteria

All bids shall be evaluated on technical and financial merit. The Company Evaluation Criteria is attached at **Annex 'D'** for reference.

BOARD OF MANAGEMENT ★ Quaid-e-Azam Industrial Estate ★
Sr. Estate Manager

7 Undertaking

On behalf of the company it is certified that we agree to the all the Instructions and Terms & Conditions given in this Bidding Document

Name of bidder…………………………………………………………………………………

Authorized person……………………………………………………………………………...

Authorized signature……………………………………………………………………………

Stamp……………………………………………………………………………………………

Office Address…………………………………………………………………………………

Tel No ……………………………………………………………………………………………

Fax No …………………………………………………………………………………………

Pmt.

BOARD OF MANAGEMENT ★ Quaid-e-Azam Industrial Estate
7
Sr. Estate Manager

Annex 'A'

PROCUREMENT, INSTALLATION, COMMISSIONING OF WIRELESS NETWORK IN QIE BUILDING

Sr. No.	Name of Articles with Specifications	Required Qty.
1	**Access Points** • Ceiling-mounted Wi-Fi AP with extended signal range. Weight With Mounting Kits: 600 g (1.3lb) Network Interface: 1GbE RJ 45 Port Ethernet Buttons Power Method: PoE Power Supply: PoE switch 48V, 0.5 A Gigabit PoE adapter Power Save Maximum Power Consumption: 13W Throughput rate: 2.4 GHz (573.5 Mbps), 5 GHz 4.8 Gbps Wi-Fi Standards: 802.11a/b/gWiFi4/WiFi5/WiFi6 Wireless Security: WPA-PSK,WPA-Enterprise(WPA/WPA2/WPA3) BSSID Up to 8 per radio **Advanced Traffic Management** VLAN: 802.1Q Advance Qos: Per-user rate limiting Guest Traffic Isolation: Supported WMM: Voice, video, best effort, and background Concurrent Clients: 300+ **Supported Data Rates** 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps 802.11b: 1, 2, 5.5, 11 Mbps 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps 802.11n: 6.5 Mbps to 450 Mbps, (MCS0 - MCS23, HT 20/40) 802.11ac: 6.5 Mbps to 867 Mbps, (MCS0 - MCS9 NSS1/2, VHT 20/40/80) 802.11ax(WiFi6): 7.3Mbpsto4.8Gbps (MCS0 - MCS11NSS1/2/3/4, HE20/40/80/160)	08
2	**24 Ports POE Gigabit Switches** 24 x 10/100 PoE Ethernet ports with SFP Ports. A switch of stack wise technologies which are a stack interconnect that allows administrator unified, highly resilient switching systems. Port Quantity: 24 Software: IP Base Stacking: Stackable PoE Compatibility: PoE RAM : 128 MB DRAM: 256 MB OSI Layer: L3 Port Speed: 10/100/1000 VLAN Ids: 4K Stacking Bandwidth: 32 Gbps Available PoE Power :370W	01

BOARD OF MANAGEMENT ★ Quaid-e-Azam Industrial Estate ★
Sr. Estate Manager
8

Sr. No.	Name of Articles with Specifications	Required Qty.
	Forwarding Rate of Switch (with two 10GbE Uplinks): 65.5 mpps Product Width: 17.5” Condition: Refurbished Warranty: At least one year local warranty	
3	**48 Ports POE Gigabit Manageable Switches** 48 x 10/100 PoE Ethernet ports with SFP Ports. A switch of stack wise technologies which are a stack interconnect that allows administrator unified, highly resilient switching systems. PoE Port Quantity: 48 Software: IP Base Stacking: Stackable PoE Compatibility: PoE RAM : 256 MB Flash Memory: 128 MB OSI Layer: L3 Port Speed: 10/100/1000 Ethernet VLAN Ids: 4K Switching Capacity: 160 Gbps Stacking Bandwidth: 32 Gbps PoE Budget: 715W Forwarding Rate of Switch (with two 10GbE Uplinks): 65.5 mpps Product Width (WxDxH): 17.5in x 18.0 in x 1.75 in Mounting Type: Rack-Mountable LED Indicators: Status, Link, Speed, Activity Power Supply: 715W AC Condition: Refurbished Warranty: At least one year local warranty	02
4	**CLOUD KEY CONTROLLER** • Fully Integrated Stand-alone Controller with 1 TB Storage • Multi-Site Network Management • Remote, Private Cloud Access **Mechanical** Dimensions 131.2 X 27.10 X 134.20 MM (5.2 X 1.1 X 5.3”) Weight: 582 g Enclosure: Anodized Aluminum **Hardware** Management Interface: Ethernet, Bluetooth Storage capacity: 1TB SSD (User upgradeable) Memory Processor: APQ8053 8 Core with 3 GB RAM eMMC Memory: 32 GB Network Interface: GbE RJ45 port Display: 1.42” Gray Scale OLED	01

BOARD OF MANAGEMENT ★ Quaid-e-Azam Industrial Estate
Sr. Estate Manager

Sr. No.	Name of Articles with Specifications	Required Qty.
	Buttons: Power; Factory Reset Certifications: FCC, CE, IC **Features:-** Multi-Site Management: Every Site is accessible through its assigned secure way Improved User Experience: Redesigned to be more intuitive and easier to navigate, the new UI raises the bar for enterprise network management efficiency. Important network details are logically organized for a simplified and powerful interface. Network Overview: Comprehensive Overview of the Network and make on the-fly adjustments as needed. Detailed Analytics: Use the configurable reporting and analytics to monitor users and expedite troubleshooting LAN/WAN Groups: Create multiple LAN and WAN groups and assign them to the respective device. Dashboard: Use a visual representation of network's status and delivers basic information about each segment Statistics: Visual representation of the network clients and network traffic carried by managed switched and Aps.	
5	**Router Board** The Router Board Supports IPsec hardware acceleration. This device will easily handle any task which have configured RouterOS to perform. All of this power, in a compact, fanless and professional looking solid material enclosure in a matte black. Following are the specifications of the router board: - **Powering** Number of DC inputs: 2 (DC Jack, PoE-IN) DC Jack Input Voltage: 12-57 V Max Power Consumption: 33W Max Power Consumption without attachments: 18 W Cooling Type: Passive PoE in: Passive PoE PoE in input Voltage: 18-57 V Ethernet 10/100/1000 Ethernet Ports: 10 Fiber SFP+Ports: 01 Peripherals Serial Console Port: RJ 45 **Other** PCB temperature monitor: Yes Voltage Monitor: Yes CPU:AL21400 Size of RAM: 1 GB Storage Size: 512MB Minimum SFP+Port: 128 MB Switch Chip: RTL8367SB Power Jack: 1 PoE in: Yes (port 1), passive, 18-57 V PoE out: Yes (port 10), passive, up to 57 V	01

Sr. No.	Name of Articles with Specifications	Required Qty.
	Voltage Monitor: Yes Serial ports: RJ45 License Level: 5 Operating System Router OS: Router OS v7 (Preinstalled & licensed), no separate purchase required, Free software updates for the life of product Accessories: Power Adapter, Rack Mount, Kit included by default accessories Certification & Approvals: CE,EAC, ROHS IP: IP20	
6	**Patch Panel-48 port** • 48-Port Patch Panel for High-Speed Cat6 Network Cabling Following are the specifications of the router board: - Product Type: Rack Mount Technology: Cat6 No. Of Ports: 48 Side A- Connector1: 110 IDC Side B- Connector1: RJ45 (Female) PoE Type: Tpye 2 PoE+(30W, IEEE 802.Sat) Panel Style: Punch Down Color: Black Product Compliance: Trade Agreements Act Warranty & Support: Lifetime Limited Warranty	02
7	**Cable Manager-48 Ports** Product Type: Rackmount No. Of Ports: 48 Technology: Cat6 Housing: Galvanized Sheet Steel, Powder Coated Black Measurements (HxWxD): 44x485x123mm	02
8	**Face Plate Single** • Corning Single Gang 1 Port Network Faceplate • Prevents dust and debris from entering ports • High-Quality plastic ensures durability and longevity • A sleek professional look enhances any installation • Easy to install with standard mounting hardware • Must be compatible with standard network keystone jacks. Following are the specifications of the Face Plate Single RJ45: - Environment: Indoor Halogen-free: yes RoHS: Free of hazardous substances according to RoHS 2011/65/EU Color: White No. Of Ports: 1 Height & Width: 86 mm x 86 mm Material: Durable Plastic	13
9	**Face Plate Double** Following are the specifications of the Face Plate Double RJ45 Environment: Indoor	38
10	**UTP Cat 6 Cable Roll** Bare Copper Wire 23AWG Conductors, ETL Verified to TIA-568.2-D Category 6 Standard, Plenum & Riser, Foot Length markers, UL & CSA Compliant, CMP & CMR Listed	07 Rolls
11	**RJ 45 Connectors** Regional Availability: Asia ANSI / TIA Category: 6	01 Box

Inl.

BOARD OF MANAGEMENT * Quaid-e-Azam Inn... Estate
Sr. Estate Manager

Sr. No.	Name of Articles with Specifications	Required Qty.
	Data Transfer Rate: 1000 Mbps Connectivity Technology: RJ45 Ethernet Gauge: 26.0	
12	**Double Section Data Rack (20 Gauge Outer / 18 Gauge Inner)** Wall mount data rack double section	02
13	**Dual band USB 3.0 Wi-Fi Receiver** Omni Directional IEEE 802.11ac, IEEE 802.11a IEEE802.11n, IEEE802.11g, IEEE 802.11b Frequency: 5GHz 2.4 GHz High Gain Wireless MU-MIMO USB Adapter Archer T4U	03
14	**Back Box**	55
15	**Patch Cord 1 Meter**	80 Mtr.
16	**I/O**	70
17	**PDU 6 Ports**	02
18	**Network Installation, Commissioning, testing Service**	01 Job

Dmt.

BOARD OF MANAGEMENT * Quaid-e-Azam Industrial Estate
Sr. Estate Manager

Annex 'B'

TECHNICAL SCOPE OF WORK

Revamping BOM QIE network infrastructure with a mix of Access Points, Router Board, Cloud key controller and manageable switches equipment (Active & Passive) will offer strong connectivity, security, and control.

Here are some key technical considerations and requirements for secure installation and optimal performance:

1. Network Security Requirements

- **Access Control**: Ensure the network supports secure access control policies, ideally with VLAN segmentation, to isolate departments or sensitive areas. Switch must supports VLANs and can enhance this.

- **Firewalling and VPN**: Use firewall capabilities in router board to secure the network perimeter and support VPNs for remote access if needed.

- **Firmware Updates**: Keep all devices up-to-date with the latest firmware to protect against vulnerabilities.

- **Secure Management Access**: For the Cloud Key and router board, configure strong passwords and limit management access (e.g., only allow access from trusted IPs).

- **802.1X Authentication**: For additional control, implement 802.1X authentication on switches and access points to prevent unauthorized access.

2. Installation Requirements and Tips

- **Access Points (APs)**: The Access Points must of those models in which offer strong range and should be positioned to avoid overlapping coverage areas too heavily. Ideally, conduct a wireless survey to optimize placement.

- **Switching Infrastructure**: With new / refurbished switches, verify port functionality and test performance beforehand. Power over Ethernet (PoE) on these switches should cover APs and VoIP phones if used.

- **Patch Panels and Cable Management**: Install patch panels and cable managers in racks to maintain organization, labelling each connection for easy troubleshooting.

- **Data Racks**: Ensure racks are installed in secure, well-ventilated areas to prevent overheating and protect against unauthorized physical access.

3. Operational Security Measures

- **Segmentation and VLANs**: Configure VLANs on switches to separate wireless, corporate, and guest networks.

- **Logging and Monitoring**: Set up logging on all network devices and integrate with a syslog server or network monitoring solution for real-time alerts and historical tracking.

- **Backup and Redundancy**: Maintain backup configurations for all devices, especially the Cloud Key controller and router board, to ensure minimal downtime in case of failure.

BOARD OF MANAGEMENT * Quaid-e-Azam Industrial Estate * Sr. Estate Manager

4. Bidding Requirements for Vendor

- **Single-Stage, Two-Envelope Bidding**: In the technical proposal, vendors have to provide detailed methodology, including:
  - Network design and equipment configuration
  - Security practices during installation
  - Post-installation testing procedures
- **Compliance with Standards**: Specify adherence to IEEE 802.11 standards for wireless, IEEE 802.3 for wired networking, and TIA/EIA standards for cabling and patch panels.
- **Certification and Experience**: Vendors must provide the list of certifications (e.g., Cisco, Access Points, Router board) and relevant experience in similar projects.
- **Warranty and Support**: Include post-installation support and warranties for all devices and Labor to ensure quick troubleshooting and repairs if needed.

Following these guidelines vendor will ensure a robust and secure network infrastructure deployment.

Load Balancing, Bandwidth Management, VLAN Segmentation & Strict Access Control

A smart network solution may incorporate in which load balancing, bandwidth management, VLAN segmentation, and strict access controls. Here's a detailed approach:

1. Dual ISP Management and Redundancy

- **Load Balancing and Failover**: Configure load balancing between PTCL and Fiber internet connection using the router board. This ensures consistent bandwidth distribution and automatic failover if one ISP goes down.
- **ISP Allocation**: To optimize usage, dedicate certain services or departments to one ISP and others to the second, with flexible failover rules in case of outages.

2. Fiber-to-Fiber Switching and Secure Areas (IT & Finance)

- **Fiber Connectivity**: Use the SFP+ ports of switch to handle fiber connections securely between ISPs and the internal network. Switch must support fiber uplinks and secure routing to designated areas.
- **VLAN Segmentation for Sensitive Areas**: Configure separate VLANs for IT, Finance, and each department along with general users. Each VLAN should have specific access permissions, ensuring sensitive data remains isolated and secure. Only devices within the IT and Finance VLANs should have access to sensitive systems.

3. Bandwidth Allocation and Control

BOARD OF MANAGEMENT * Quaid-e-Azam Industrial Estate
Sr. Estate Manager

- **User-Specific Bandwidth Management**: Use the router's built-in QoS features to assign and monitor bandwidth limits per user or department. Set up bandwidth caps for general users while prioritizing IT, Conference Room, President Room and Finance-Accounts Dept. VLANs.

- **Guest Wi-Fi with Limited Bandwidth**: Configure a separate SSID for guests on access points, allocating minimal bandwidth. Set up captive portal access to ensure that each guest agrees to terms before accessing the network.

- **Dynamic Bandwidth Allocation**: Router features also allow for dynamic allocation based on current network demands, which can help optimize the usage further during peak times.

4. Access Control and Monitoring

- **Access Point Restrictions**: Set up centralized control of access points through the Cloud Key. With a role-based administration setup, ensure only IT administrator can access and modify configurations.

- **Access Logs and Monitoring**: Enable logging on both the router and switches to monitor access to the IT and Finance VLANs. Regularly review access logs for any unauthorized attempts.

- **Role-Based Access**: Implement strict role-based access to network devices, allowing only admin-level users to make any network modifications. For physical security, install data racks in secure, access-controlled rooms.

5. Network Monitoring and Security

- **Centralized Monitoring and Alerts**: Use the Cloud Key and Router board monitoring tools to oversee access points, bandwidth usage, and potential network intrusions. Automated alerts can notify you of unusual activity in sensitive VLANs.

- **Firewall Rules for VLANs**: Use Router board firewall features to establish rules that restrict inter-VLAN communication, particularly isolating the guest network from corporate traffic.

6. Vendor Implementation Requirements

- **Clear SLA**: Require the vendor to set up and test load balancing, VLANs, and bandwidth control configurations and ensure they match QIE security and performance needs.

- **Post-Installation Support**: Set up post-installation support to help fine-tune bandwidth allocations and address potential issues as your network load fluctuates.

This solution maximizes ISP redundancy, provides secure segmented access, and ensures that each user and guest has defined, controlled bandwidth.

IP Scheme for Wired & Wireless System

A well-planned IP scheme is essential for organized network management, efficient troubleshooting, and scalability. For BOM-QIE setup, using a private IP addressing scheme with subnetting will be ideal. Here's a suggested IP scheme:

1. IP Addressing Scheme Overview

Pmt.

- **Private IP Range**: Use the 10.0.0.0/8 or 192.168.0.0/16 range, as these provide ample IPs and allow for flexible subnetting.

- **Subnetting**: Subnet by department or purpose (e.g., IT, Finance, General Users, and Guest Wi-Fi). This helps in applying access control and tracking network traffic.

2. Proposed Subnetting and IP Assignments

- **10.0.0.0/8 IP Range**: This range allows for easy expansion and segmentation, and using a Class A network also enables subnets for each VLAN without IP conflicts.

VLAN/Network	IP Subnet	Subnet Mask	Purpose
Core Network (IT)	10.0.1.0/24	255.255.255.0	Internal IT systems, servers
Finance Network	10.0.2.0/24	255.255.255.0	Finance department devices
General Users (Wired)	10.0.3.0/24	255.255.255.0	General employee wirednetwork
Wireless Network (Staff)	10.0.4.0/24	255.255.255.0	Staff wireless devices
Guest Wi-Fi	10.0.5.0/24	255.255.255.0	Guest wireless network (limited)
Management VLAN	10.0.6.0/24	255.255.255.0	Access points, switches, routers
Printers/IoT Devices	10.0.7.0/24	255.255.255.0	Networked printers, IoT devices

3. Address Allocation for Each Network

- **Gateway (Router)**: Use the first IP in each subnet for the gateway (e.g., 10.0.1.1 for IT, 10.0.2.1 for Finance).

- **Static Devices**: Allocate static IPs for servers, switches, and network devices within the first few IPs of each subnet (e.g., 10.0.1.2-10.0.1.20 for IT servers).

- **DHCP Scope**: Use DHCP for general users and staff devices, defining a range within each subnet (e.g., 10.0.3.50-10.0.3.200 for wired users).

4. Implementation Notes

- **Routing and VLAN Setup**: Use router board to set up VLANs with inter-VLAN routing where necessary. Configure firewall rules to restrict communication between VLANs, especially for Guest Wi-Fi.

- **Access Point IPs**: Place all APs on the Management VLAN, giving them IPs like 10.0.6.10, 10.0.6.11, etc. Only IT admins should have access to this VLAN.

Ind.

- **Bandwidth and Security Controls**: With this scheme, applying Router board bandwidth management and VLAN-specific firewall policies becomes easier.

This tentative structure provides clarity and allows for seamless management of devices while securing sensitive networks. Except this solution, a vendor may submit a better & secure solution.

MAC Based Controls

Locking devices by MAC address can be effective for security but may also add administrative overhead. Here's a breakdown of when and how to consider MAC-based controls:

1. When to Use MAC Address Locking

- **Sensitive Areas (e.g., IT and Finance)**: Locking MAC addresses in these areas can add a layer of security by ensuring only registered devices can connect, which is useful for departments handling sensitive data.

- **Wired Connections**: Locking MAC addresses for wired connections is generally more manageable, as devices are stationary, and there's less risk of MAC address changes.

- **Guest Wi-Fi Network**: You can skip MAC address locking on the guest network, as guest devices vary and should have limited access regardless.

2. Advantages of MAC Address Locking

- **Added Security**: It restricts access to known devices, reducing the chance of unauthorized access, especially helpful in sensitive areas like servers and PCs.

- **Control Over Network Devices**: This ensures that only organization-approved devices can connect, which helps keep unknown devices off your network.

3. Drawbacks of MAC Address Locking

- **Increased Administrative Load**: Every time a new device needs access, IT staff will have to update the MAC address list, which can be time-consuming.

- **MAC Spoofing Vulnerability**: Although MAC locking adds a layer of security, determined attackers can still spoof MAC addresses if they know an allowed MAC address on the network.

- **Device Management**: Users may change devices or add new devices frequently (especially for wireless), which could complicate management.

4. Best Practices if Implementing MAC Locking

- **Combine with Other Security Measures**: Use MAC locking alongside VLANs, firewalls, and user authentication for comprehensive security.

- **Limit to Key Devices**: Lock only high-priority devices (e.g., IT and Finance department computers and important servers) rather than every user's laptop or mobile device.

BOARD OF MANAGEMENT ★ Quaid-e-Azam Industrial Estate

Sr. Estate Manager

- **Regular Review**: Periodically review and update the MAC address list to ensure it's current and does not hinder productivity.

Recommended Approach

For our (BOM-QIE) setup, it's practical to lock MAC addresses only for:

- **Critical devices in IT and Finance**

- **Wired desktops or PCs that don't frequently change**

For general wireless devices (laptops, mobile phones), consider skipping MAC locking but implement strong Wi-Fi security protocols like WPA3, VLANs, and device isolation. This approach balances security with ease of management.

Network Monitoring (Usage analytics)

As an IT administrator, to maintain the check and balance of network usage analysis, we must monitor user activity and track network tasks effectively within this setup. Here are suggested methods to help us monitor users and gain insights into network usage while respecting privacy and security policies:

1. Network Monitoring Tools and Software

- **Router board Logs and Traffic Flow**: Router's support features like traffic flow monitoring, which can help track the volume and direction of data each user is consuming. By enabling Router board Traffic Flow or NetFlow, admin can approach the log data about IP connections, helping to see which services or websites users are accessing.

- **Unified Network Management**: Controller (Cloud Key) allows for centralized logging and monitoring of access points, showing which users are connected, connection times, and the amount of data transferred per device. This is useful for wireless tracking.

- **Syslog Server**: Direct logs from network devices (switches, routers) to a syslog server, which aggregates and stores logs for analysis. This will let us review logs over time to detect usage patterns, network anomalies, and specific actions.

2. Bandwidth and Application Usage Monitoring

- **Bandwidth Management and QoS**: Use the router's Quality of Service (QoS) feature to monitor and allocate bandwidth. By analyzing bandwidth usage, you can identify high-demand users and manage it accordingly. Router's Queue Tree can also show which users or applications are consuming the most bandwidth.

- **Deep Packet Inspection (DPI)**: Tools like Router's Layer 7 protocol can help in identifying traffic by application type, which enables IT Administrator to see which services (like streaming, social media, or file downloads) are being accessed.

3. VLAN-Based Monitoring for Specific Departments

BOARD OF MANAGEMENT ★ Quaid-e-Azam Industrial Estate
Sr. Estate Manager

- By configuring VLANs, IT Administrator can monitor traffic per department or sensitive area (e.g., IT and Engineering, Finance) and observe specific user activity within those VLANs. This approach lets the IT dept. identify unusual patterns or potential security breaches more easily by department.

4. Employee Device Tracking with MAC Address Locking and IP Assignment

- Since each device can be assigned a static IP within a VLAN, monitoring tools can log activity by IP address, effectively linking user actions to individual devices. For example, if a Finance user has a specific IP, any access to sensitive data can be traced to that IP.

5. User Authentication and Logging

- **RADIUS Server Authentication**: By using RADIUS (Remote Authentication Dial-In User Service) for wireless and VPN access, IT Dept. can authenticate users individually and track session data, such as login times and network resource usage.

- **Captive Portal for Guest Network**: Configure a captive portal on the guest Wi-Fi that requires users to log in before access. This helps IT Dept. monitor and restrict access while logging guest activities.

6. Third-Party Network Monitoring Solutions

- Consider third-party solutions like SolarWinds, PRTG, or Nagios for more granular monitoring and reporting. These tools provide detailed user activity logs, application monitoring, and alerting, which can enhance the visibility over the network.

Important Considerations

While monitoring user activity is possible, it's essential to:

- **Ensure Compliance with Privacy Policies**: Obtain necessary permissions and be transparent about monitoring policies with users.

- **Limit to Necessary Monitoring**: Focus on tracking network usage and application types rather than specific browsing details, respecting users' privacy where possible.

- **Secure Monitoring Data**: Store monitoring data securely, as it may contain sensitive information.

With this setup, IT Dept. can effectively monitor user tasks, bandwidth usage, and activity patterns, providing insights that help manage the network more proactively.

Management of Resource Sharing (Hardware)

To manage printing access efficiently within our network, you can set up each printer based on department needs and access controls. Here's a practical solution for your setup:

1. Konica Minolta Bizhub 450i Photocopier (Organization-Wide Access)

- **Network Setup**: Place the Bizhub 450i on the **General Users VLAN** with a static IP address (e.g., 10.0.3.10). This allows it to be accessible by all users on the network.

BOARD OF MANAGEMENT
Estate Manager
Quaid-e-Azam Industrial Estate

- **Driver Installation and Configuration**: Ensure all user devices (PCs, laptops, and mobile phones) have the necessary drivers installed to connect to the Bizhub 450i. The printer should support mobile printing via Wi-Fi Direct or a mobile app, so check if a mobile app is required for easier access.

- **Access Controls**: Use the Konica Minolta's built-in user authentication feature to track who is using the copier. This helps manage usage and prevents unauthorized access.

- **Print Management Software** (Optional): If tracking and quotas are important, consider adding print management software like Papercut or Uniflow etc. These tools can integrate with network printers and provide usage reports.

2. HP 402Dnw Printer (Finance Dept. | Engineering Dept. | Admin Dept.)

- **Network Placement**: Connect the HP 402Dnw to the **Finance VLAN** (e.g., assign IP 10.0.2.20)& So on. This keeps it isolated from general users but accessible by Finance staff& So on.

- **Wireless Printing**: The HP 402Dnw supports wireless printing, so Finance users can connect directly via Wi-Fi. Set up the printer's Wi-Fi settings and distribute the connection details (SSID and password) to Finance staff only.

- **User Access Control**: Configure the printer to accept connections only from approved MAC addresses of Finance department devices for additional security.

3. Accounts Department Central Network Printer (Finance and Accounts Only)

- **Network Placement and Access Control**: Connect this printer to a shared **Finance/Accounts VLAN** (e.g., 10.0.8.0/24), allowing only these departments to access it. Assign a static IP (e.g., 10.0.8.10) and restrict access to that VLAN.

- **Printer Sharing Setup**: Enable network sharing on this printer so that it's accessible only to users within the specified VLAN. This ensures that users from other departments cannot view or connect to this printer.

4. Network and Security Considerations

- **Firewall Rules**: Configure firewall rules on the MikroTik router to allow printer access only to designated VLANs. For instance, restrict Bizhub 450i access to the General User VLAN, HP 402Dnw to the Finance VLAN, and the Accounts printer to the Finance/Accounts VLAN.

- **Device Isolation**: Enable device isolation within VLANs as needed, especially for wireless users, so that only devices with permissions can connect to each printer.

- **Driver Distribution**: Ensure that drivers for each printer are accessible via a shared network folder or intranet portal, simplifying user setup.

This approach segments printers by department, ensures secure access, and keeps the network organized. Let me know if you need specific details on configuring firewall rules or printer drivers!

Network Remote Controlling

As the network administrator, it is necessary to set up remote management to control and monitor this network

BOARD OF MANAGEMENT * Quaid-e-Azam Industrial Estate *
St. Estate Manager

from any location. Here are secure ways to do this:

1. <u>**Use VPN for Secure Access**</u>

- **VPN Setup on Router**: Vendor must Configure a VPN (Virtual Private Network) on thecentral router to provide encrypted access to the organization's network. This will allow administrator to securely connect to this network from outside, ensuring encrypted access to internal resources as if administrator were on-site.

- The VPN should support secure protocols like OpenVPN, L2TP/IPSec, or WireGuard etc.

- **Remote User Authentication**: Use strong authentication methods (like two-factor authentication) to secure VPN access, which is critical for protecting against unauthorized remote access and managed centrally by the IT dept. Vendors must implement MFA for all remote access points, including:

  - VPN login.
  - Access to shared drives and email servers.
  - Cloud backups and administrative panels.
- MFA options can include OTP-based apps (e.g., Google Authenticator) or hardware tokens or any other.

2. <u>**Remote Management of Devices**</u>

- **Router WinBox or WebFig**: With VPN enabled, admin can use Router's WinBox or WebFig remotely to manage router configurations, monitor traffic, and check firewall rules.

- **Controller (Cloud Key)**: As we have the Cloud Key, admin can access the Controller remotely by enabling Remote Access in the Cloud settings. This allows admin to monitor and manage access points, track user connections, and configure network settings.

- **Secure SSH Access**: For routers and switches, enabling SSH access (restricted to specific IPs) provides secure, command-line-based control from any location.

3. <u>**Remote Desktop Access**</u>

- **RDP or VNC**: Bidder must Set up remote desktop access to a central workstation on the network (secured by VPN). This workstation can act as our primary management hub, from where admin can access network devices and monitor network activity.

- **Centralized Management Software**: Tools like TeamViewer or AnyDesk provide secure, Google Desktop Connection through Code Generation (renew on every visit) on-demand access to our networked devices, with options for encrypted connections and session logging.

4. <u>**Security Best Practices for Remote Access**</u>

- **IP Whitelisting**: Limit access to known IP addresses where possible to minimize exposure.

- **Firewall Rules**: Set up firewall rules on router to restrict remote access ports and protocols, only allowing necessary traffic.

- **Regular Monitoring and Alerts**: Set up alerts for any unusual activity or failed login attempts on critical network devices to detect and respond to potential security issues quickly.

BOARD OF MANAGEMENT ★ Quaid-e-Azam Industrial Estate
Sr. Estate Manager

5. Monitoring and Logging

- **Syslog Server and Remote Logging**: Configure a syslog server that admin can access remotely. This provides a centralized view of network logs for troubleshooting and monitoring.

- **SNMP for Alerts**: Use SNMP (Simple Network Management Protocol) to receive alerts on critical network events, which can be configured to notify admin via email or SMS when specific thresholds or incidents occur.

- **File Access Protocols**: Use secure file-sharing protocols such as SFTP or SMB with encryption enabled.

- All data transmitted between the server and remote devices must be encrypted using SSL/TLS.

With these steps, we'll be able to securely manage this building network remotely, keeping it functional and secure from any location.

To ensure users can work safely from home and access the organization's network, the following procedures should be adopted by the bidder. These measures will guarantee secure, reliable remote access while maintaining the integrity of the system:

6. Bandwidth Management

- **Bandwidth Allocation**:

o Use QoS (Quality of Service) to allocate sufficient bandwidth for remote users without compromising on-site operations.

- **Guest Wi-Fi Isolation**:

o Ensure the guest Wi-Fi network remains isolated from work-related remote access traffic.

7. Vendor Support Requirements

- **Live Support**: Vendors must offer 24/7 remote support for troubleshooting connectivity and security issues.

- **Emergency Protocols**: Establish emergency response protocols to address remote access failures or security incidents.

These procedures will ensure seamless and secure remote access for users, enabling productivity while maintaining the network's security.

Centralized Email Setup in this Network

1. Centralized Management:

- All email data will be stored on a dedicated server, making it easier to manage, back up, and secure.
- IT staff / admin can centrally configure storage quotas, access permissions, and recovery policies.

2. Data Security:

- Central storage reduces the risk of losing email data due to individual system crashes.
- The server can be configured with robust security measures, such as restricted access and encryption.

BOARD OF MANAGEMENT * Quaid-e-Azam Industrial Estate
Sr. Estate Manager

3. **Backup and Recovery**:

- A centralized server allows for automated backups of all .pst files, ensuring that no email data is lost in case of accidental deletion or corruption.
- Easier disaster recovery compared to restoring individual user machines.

4. **Improved Performance on User Devices**:

- Storing .pst files on a server prevents email storage from consuming local disk space on user devices.
- Reduced load on local hardware can improve the overall performance of user PCs.

5. **Simplified IT Support**:

- Centralized email storage reduces the complexity of managing scattered .pst files on individual devices.
- Migration to new systems or restoring data becomes quicker and more reliable.

6. **Standardized Email Experience**:

- Consistency in email storage across the organization ensures uniform performance and functionality.

Bidder shall confirm the email centralization using this networking system. As already Outlook on Every user's PC has been configured, the master file will be stored in Centralized server which will be located in IT dept.

Data Storage & Backup

To ensure the data storage and backup system is secure and operational, the following safe instructions should be provided to the bidders:

General Instructions

1. **Compliance with Standards**:

o Bidder(s) must comply with industry best practices and standards, such as ISO/IEC 27001 for data security.

2. **Bidder Accountability**:

o Bidders must ensure proper documentation of all configurations, including server directories, user permissions, and backup schedules.

o Any modifications or deviations from the agreed plan must be approved by the IT administrator.

Local Server and Shared Drive Configuration

1. **User Data Storage**:

o Each user must be assigned a unique directory on the centralized server, accessible only with their username and password.

o The shared drive must have strict access controls to prevent unauthorized modifications or deletions.

2. **Access Permissions**:

o Set role-based permissions for directories to ensure users can only access their data.
o Shared drives should have read/write restrictions based on roles and departments.

3. **Encryption**:

BOARD OF MANAGEMENT
Quaid-e-Azam Industrial Estate
SA Estate Manager

- All data stored on the server must be encrypted both at rest and in transit using protocols like AES-256 and TLS.

4. **Server Hardening**:

- Disable unnecessary services, ports, and protocols on the server.
- Regularly update server firmware and operating systems to address vulnerabilities.

Backup Policies

1. **Local Backup**:

- Daily incremental and weekly full backups must be configured for all user directories and shared drives on external disk drives.

- Vendors must use backup software capable of scheduling automated backups.

2. **External Backup Verification**:

- Backups on external drives must be verified for integrity and completeness before overwriting older versions.

3. **Cloud Backup Integration**:

- Configure automatic synchronization between external portable drives and the selected cloud storage solution once purchased.

- Cloud data must be encrypted before transmission to ensure security.

Monitoring and Reporting

1. **Audit Logs**:

- Enable detailed audit logging for access, changes, and backups on both the local server and external drives.

- Provide logs to the IT administrator weekly or upon request.

2. **Failure Alerts**:

- Implement automated alerts for backup failures, unauthorized access attempts, or system errors.

3. **Vendor Support**:

- Ensure the bidder provides 24/7 support for troubleshooting and system restoration.

Security Safeguards

1. **Firewall and Antivirus**:

- Configure firewalls on the local server to restrict external access.

BOARD OF MANAGEMENT ★ Quaid-e-Azam Industrial Estate ★
Estate Manager

o Install and configure antivirus software (will be provided by the procuring agency) to scan server directories regularly.

2. **User Authentication**:

o Enforce multi-factor authentication (MFA) for server access.

o Passwords must meet strong complexity requirements and be changed every 30 days.

3. **Physical Security**:

o The server and external backup drives must be stored in a secure IT room with access restricted to authorized personnel.

4. **Data Retention**:

o Define data retention policies, such as storing backups.

Testing and Training

1. **Testing Phase**:

o Bidders must demonstrate the functionality of the local server, shared drives, and backup systems before final handover.

o Perform mock restores to ensure backup data is retrievable.

2. **User Training**:

o Provide training to IT administrators on managing server directories, backups, and cloud integrations.

3. **Handover Documentation**:

o Deliver complete system documentation, including network topology, server configuration, and backup schedules.

These instructions to bidders will ensure a secure, robust, and operational data storage and backup system in this networking system. Furthermore, one (01) Photocopier machine (Konica Minolta) will be shared to all users of every department. Also, there are Two (02) Biometric IP based machines ZKteco MB460 & ZKteco Uface 800 plus which is in operational by the HR & IT dept. & bidder have to also synchronize these machines in network.

Finally, providing the building map to bidders will be crucial for planning network topology, access point placement, and cable routing.

BOARD OF MANAGEMENT ★ Quaid-e-Azam Industrial Estate ★
Sr. Estate Manager

Annex "C"

PROCUREMENT, INSTALLATION, COMMISSIONING OF WIRELESS NETWORK IN QIE BUILDING

(Bid Form)

Sr. No.	Name of Articles	Required Qty.	Unit Price (Inclusive of all taxes) PKR	Total Price (inclusive of all taxes) PKR
1	Access Points	08		
2	24 Ports POE Gigabit Switches	01		
3	48 Ports POE Gigabit Manageable Switches	02		
4	CLOUD KEY CONTROLLER	01		
5	Router Board	01		
6	Patch Panel-48 port	02		
7	Cable Manager-48 Ports	02		
8	Face Plate Single	13		
9	Face Plate Double	38		
10	UTP Cat 6 Cable Roll	07 rolls		
11	RJ 45 Connectors	01 Box		
12	Double Section Data Rack (20 Gauge Outer / 18 Gauge Inner)	02		
13	Dual band USB 3.0 Wi-Fi Receiver	03		
14	Back Box	55		
15	Patch Cord 1 Meter	80 Mtr.		
16	I/O	70		
17	PDU 6 Ports	02		
18	Network Installation, Commissioning, testing Service	01 Job		
			Total Price (Inclusive of all Taxes) in Figures	

Total Price (Inclusive of all Taxes) in Words	

BOARD OF MANAGEMENT ★ Qua[illegible]m Industrial Estate
St. Estate Manager

Annex 'D'

Evaluation Criteria

1. Basic Evaluation Criteria

i. Profile of company complete in all respect.

ii. List of Previous and Current customers, Purchase Orders should be attached with technical bid.

iii. Legal registered entity (Sole Proprietor, Registration with SECP or Registrar of Firm) having valid NTN, GST and PST if applicable

iv. Complete Income Tax Returns for Last three fiscal Years

v. An affidavit on Rs 100/- Stamp Paper issued after date of publishing of Tender Notice/Invitation to Bid which illustrate that currently they are not black listed or de-barred by any Government/Semi- Government Department/ Autonomous Body to participate in bidding. Failure to submit such affidavit may lead to disqualification.

vi. Details of all the items & specifications provided by supplier against items detailed as given at **Annex 'A'**

vii. Acceptance of technical scope of work as provided in **Annex 'B'**

viii. Proposed delivery schedule for delivery of items.

ix. Signed and Stamped Complete bidding document.

x. Bank Draft of the Bid Security attached with technical proposal estimated cost mentioned in the Tender notice/Invitation to Bid.

xi. Minimum 1 to 3 years' experience (Firm must attach five related supply orders as a proof withthe technical bid)

Note: Basic Evaluation Criteria is mandatory to fulfill to qualify for detailed evaluation. Failure to meet and submit all documents along with Bidding Documents on EPADS related to basic evaluation may lead to disqualification.

BOARD OF MANAGEMENT * ...strial Estate
Sr. Estate Manager

2. Detailed Evaluation Criteria

(Minimum Passing Score required is 65 Points for qualifying to Financial Opening)

DETAILED EVALUATION CRITERIA FOR

Specifications are available at Annex-A

Sr. No	Item Name and Description	Marks	Max Marks
1	**Company having Experience from the date of its incorporation**	--	10
1.1	1 – 3 years of incorporation.	2	--
1.2	4 – 6 years of incorporation.	4	--
1.3	7 – 10 years'of incorporation.	6	--
1.4	Above 10 years of incorporation	10	--
2	**Relevant Work Experience**	--	15
2.1	1-3 Purchase Orders of related work	5	
2.1	4– 6 Purchase Orders of related work	10	--
2.2	Above 6 Purchase Orders of related work	15	--
3	**Cumulative Annual Financial Turnover of Bidder as per income tax returns for Last three fiscal Years**	--	20
3.1	01 Million to 5 Million	5	--
3.2	Greater than 5 Million	10	
3.3	Greater than 10 Million	20	
4	**Technical Evaluation of quoted items**	--	55
4.1	Specification of items offered should matched as provided in Annex-A.	20	
4.2	Data Sheets (Literature) attached as per Specification of items offered	10	
4.3	Satisfactory letter from at least 3 end users/Clients during last 2 fiscal years	15	
4.4	Guarantee / Warranty provided as per specification of items requirement	10	
Total		**--**	**100**

★ BOARD OF MA[illegible]GEMENT ★
Sr. Estate Manager
Quaid-A-Azam Industrial Estate