



CYBER SECURITY FOR DIGITAL PAKISTAN / NCERT

(NATIONAL CYBER EMERGENCY RESPONSE TEAM)

TENDER DOCUMENT

Establishment of Cyber Operations & Defense Emulation Lab

GOVERNMENT OF PAKISTAN
CYBER SECURITY FOR DIGITAL PAKISTAN/nCERT
(NATIONAL CYBER EMERGENCY RESPONSE TEAM)

INVITATION TO BIDS

1. Cyber Security for Digital Pakistan /nCERT invites bids for “**Establishment of Cyber Operations & Defense Emulation Lab at National CERT**” under the “Project Cyber Security for Digital Pakistan/nCERT” for which electronic bids are invited in accordance with PPRA Rules under the Single Stage Single Envelope bidding procedure from the firms/companies registered with Income Tax, Sales Tax Departments and who are on FBR’s Active Taxpayer’s List (ATL) through e-PADS.
2. The prospective service providers are required to submit their electronic bids including technical and financial proposals along with the Bid Security instrument amounting to Rupees Eight Hundred Thousand Only (“PKR 800,000 only”) submitted in favor of Project Director PKCERT (FTN/NTN: 9012000-7) through e-PADS at <http://eprocure.gov.pk> uploaded on or before 1100 hours on 27th April, 2026 in accordance with the provisions of PPRA Rule 36(b) and other terms & conditions as defined in the bidding documents.
3. In case of any technical difficulty in using e-PADS, prospective bidders may contact PPRA team Director MIS Room No. 109, 1st floor, FBC building Sector G-5/2, Islamabad (Contact No. 051-111-137-237).
4. Original Bid security instrument MUST be submitted to the undersigned before closing hours of the bid submission time otherwise respective bid will not be opened.
5. Bidding documents can be accessed from the website of National Computer Emergency Response Team (<https://pkcert.gov.pk/>) as well as on PPRA website.
6. Bids will be opened on the same day i.e., 27th April, 2026 at 1130 hours in the presence of representatives of the bidders.
7. As per PPRA Rules 33(1), 2004, National Computer Emergency Response Team (nCERT) has the right to reject any or all bids/ proposals at any time prior to the acceptance of a bid/proposal.

Project Director
National Computer Emergency Response Team (nCERT)
L- Block, Pakistan Secretariat, Islamabad
Ph No. 051-9203421-22
Email: bid@pkcert.gov.pk
Website: (<https://pkcert.gov.pk>)

**TERMS OF REFERENCE (TOR) REQUEST FOR PROPOSAL FOR
SUPPLY OF HARDWARE AND LICENSED SOFTWARE**

1.	Background
2.	General Terms & Conditions
3.	Implementation & Payment Schedule
4.	Evaluation Criteria
5.	Award Of Contract
6.	Mailing address/ Contact information
7.	Annexure-Bill of Quantities
8.	Annex-I

1. BACKGROUND:

“Cyber Security for Digital Pakistan”, is a PSDP project sponsored by Ministry of Information and Technology (MoITT) and executed by National Telecommunication & Information Technology Security Board (NTISB). The project “Cyber security for Digital Pakistan” is a prerequisite for the Digital Pakistan initiative addressing current National cyber security gaps and concerns. This project will provide cyber security and digital initiative support to all public/private/defense sector organizations/institutes at national level. “National CERT” is a PSDP Project sponsored by Ministry of Information and Technology (MoIT&T) and executed by National Telecommunication & Information Technology Security Board (NTISB). The Project “Cyber Security for Digital Pakistan” is a prerequisite for the Digital Pakistan initiative addressing current National Cyber Security requirements. This project will provide Cyber Security support to all Public / Private / Defense Sector Organizations/ Institutions on National Scale. In pursuance, Project Director is looking to procure Security Screening Software and Hardware for PKCERT HQ’s Office at Block-L Pakistan Secretariat Islamabad.

2. GENERAL TERMS & CONDITIONS:

- i. **Proposal Submission:** The electronic bid including technical and financial proposals must be submitted online on or before 27th April, 2026 at 1100 hours through e-PADS at <http://eprocure.gov.pk>.
- ii. A bid security, in the shape of a Bank Draft / Pay Order in the name of **Project Director, PKCERT**, amounting to Rs. 0.8 million PKR should be submitted along with the Technical and Financial Proposals at the address given below latest by 27th April, 2026 at 1100 hours. Technical bids will be opened on the same date at 1130 hrs:

Project Director
Cyber Security for Digital Pakistan (CSDP/nCERT)
L- Block Pak Secretariat, Islamabad
Ph No. 051-9203421-22
Email: bid@pkcert.gov.pk

- iii. **Scope of Work:** The scope of work includes Supply, Installation and successful testing of the Hardware & Software (Indigenous) License mentioned at Annexure-I.
- iv. **Bidders** may participate in the tender under the Single Stage Single Envelope procedure and may quote for a single Lot or all Lots on a turnkey basis. Evaluation shall be carried out on an item-wise in each lot basis to ensure transparency, fairness, and competitive procurement. Each item in lot is listed in Annex-I shall be evaluated separately based on a predefined technical scoring criterion, including compliance with specifications, technology offered, OEM credentials, warranty/support, and value-added features. Only technically responsive bids achieving the minimum qualifying technical score shall proceed to financial evaluation. Financial evaluation shall be conducted item-wise among technically qualified bidders, and award of contract shall be made to the bidder obtaining the highest combined score (technical + financial) as per the approved evaluation

methodology.

- v. The bidder(s) winning each respective Lot, in accordance with PPRA Rules under the Single Stage Single Envelope procedure, shall be responsible for the complete supply, installation, configuration, integration, testing, commissioning, and handover of the respective item(s) on a turnkey basis.
- vi. Bidders shall quote item-wise prices within each Lot. Each Lot shall consist of multiple items as defined in Annex-I, and bidders must provide separate unit prices and total prices for each item. The financial evaluation shall be conducted on an item-wise and Lot-wise basis. The total Lot price shall be calculated as the sum of all item-wise prices within that Lot.
- vii. Soon after technical evaluation, the technical qualified firms as per evaluation criteria mentioned at para 4(b), shall be called for opening of financial bid on given date and time which will be communicated to the firms in writing. Un-opened bid security instrument shall be returned to the technically disqualified firms.
- viii. Proposal and prices shall remain valid for a period of 90 days from the date of closing for submission of the proposal. However, the responding organizations are encouraged to state a longer period of validity for the proposal.
- ix. Prices should be quoted in the Pakistani rupees (PKR) and inclusive of all taxes, prices mentioned without any remarks will be treated as inclusive of all applicable taxes.
- x. Any proposal received after the due date and time will not be accepted.
- xi. Bidders should be registered with Sales Tax registration Department and should be in possession of valid NTN number. Copies of the certificates must be attached with the technical bid
- xii. The successful bidders shall be responsible for payment of any duties / taxes etc. that are imposed by the Government of Pakistan during the period of delivery and till commissioning.
- xiii. The bidders are hereby informed that the Government shall deduct tax at the rate prescribed under the tax laws of Pakistan, from all payments for Hardware/Software by any bidder who signs a contract with the Government.
- xiv. The successful Firm shall be required to deposit in the form of a Bank Guarantee, a Performance Bond from the date of successful testing and acceptance, a sum equivalent to ten percent (10%) of the contract value. This Bank Guarantee shall be issued by a scheduled bank operating in Pakistan and shall be kept valid from the date of issue, until one (1) year after all contractual obligations have been fulfilled
- xv. Bidders should have been in the IT business, Sales and After Sales Support/Maintenance provisioning for at least (03) three years.
- xvi. Hardware equipment should have minimum one (01) year warranty (unless stated otherwise in Annex-I), including parts and maintenance after the delivery of hardware with next Business Day Part Replacement and on-site support. Supplier to share list of

OEM warehouses for spare-parts and accessories within the country where applicable (nCERT reserves the right to keep faulty Hardware/Equipment under parts replacement warranty claim). Software licenses should be quoted for at least 01 year with perpetual subscription option (if applicable).

- xvii.** The bidders should be authorized Partner / Reseller / Distributor / Manufacturer, of THE ORIGINAL MANUFACTURER, in Pakistan.
- xviii.** All equipment should be supplied through verifiable and legitimate distribution/Sales 6 channels.
- xix.** The Bidders to provide Company information as per para 4 for Technical Evaluation.
- xx.** Bidders should not submit any kind of refurbished/ Used / End of Life Hardware equipment's / components in their technical proposals.
- xxi.** Bidders should clearly indicate the timeline for delivery of equipment after receiving the award of contract.
- xxii.** The end user licenses, end user warranties and end user contracting support services registrations and subscriptions will be in the name of Client, for all the equipment and Software loaded on the equipment delivered during the course of this procurement. All items/solutions must be pre-configured with all applicable licenses, subscriptions and dependencies with no compatibility conflicts / missing dependencies.
- xxiii.** Envelope for financial proposals should be clearly marked: "Financial Proposal".
- xxiv.** Main Envelope should contain "Technical Proposal" & "Financial Proposal" (each being physically separated, bound, sealed and labeled), all the supporting documents as per evaluation criteria mentioned at para 4 & 2 (vi) and a separate clearly marked sealed envelope of bid security instrument.

3. IMPLEMENTATION & PAYMENT SCHEDULE:

Sr. No.	Milestones	Time Period	Payment
1.	Supply of equipment / Software. Installation and Configuration	Four-to-twelve weeks from date of signing of contract	40%
2.	Successful testing and acceptance	Four (04) weeks from installation and configuration of Hardware and Software	60% Subject to provision of 10% Performance Guarantee
3.	End of performance Guarantee	Performance Guarantee will have to be provided to cover the warranty period of the hardware which will be One year from the date of successful testing and acceptance.	Release of Performance Guarantee

4. EVALUATION CRITERIA

a. TECHNICAL BID EVALUATION:

There will be a two-stage evaluation. Preliminary evaluation (Initial Screening) of technical bids will be done on the basis of the following criteria:

Detailed technical evaluation will be done for firms who qualify the preliminary evaluation mentioned above.

In detailed technical evaluation the Evaluation & Award Committee will verify the compliance with specifications mentioned in Annexure-I. Any bid containing less specifications will be rejected.

GENERAL & TECHNICAL EVALUATION				
Sr#	Compliance	Criteria	Max Score	Obtained Score
1	Company Presence in Pakistan	Head Office in Pakistan (5) Branch Office in Pakistan (3) Partner in Pakistan (2)	5	
2	Company presence in Islamabad/ Rawalpindi	Head Office in Isl/Rwp (10) Branch Office in Isl/Rwp (7) Partner in Isl/Rwp (5)	10	
3	Working in IT business (at least 5 x years)	5 or more than 5 years exp (10) Less than 3-5 years exp (6)	10	
4	Experience of at least 3 x similar size projects	3 or more than 3 projects completed (10) Less than 3 projects completed (5)	10	
5	Solution Presentation, Demonstration and understanding of the required software/ hardware solution.	Deployment plan and functional requirements as per Annex-I	25	
6	Ranking of Technology in Gartner or other relevant body.	Leader (10) Visionary (5) Challenger (4) Niche Player (3) Others (2)	10	
7	Baseline Configuration (Anex-I)	Configuration and Specs higher than Baseline (15), Equivalent (10)	15	
8	Duration of licenses	Perpetual (10) More than 1 year (6) 1 year (4)	10	
9	Warranty duration	More than 1 year (5) 1 year (3)	5	
Total			100	

$$\text{Technical Evaluation Score (70\%)} = \frac{\text{Marks Obtained}}{100} \times 70$$

b. FINANCIAL BID EVALUATION (30%):

Financial bids of the technically qualified firms will be opened before the representatives who wish to attend the tender opening. Financial bids will be opened only for those vendors only who qualify (meet the specifications) in technical and detailed technical evaluation.

Financial Evaluation Score (30%) = $\frac{\text{Amount quoted by the lowest bidder}}{\text{Amount quoted by the bidder whose financial score is to be calculated}} \times 30$

c. Final Evaluation

Final Score (100%) = Technical Evaluation Marks (70%) + Financial Evaluation Marks (30%)

The bidders need to score at least 70% marks in technical evaluation to technically qualify for financial bid opening. The bidder scoring maximum marks in final evaluation will be awarded the contract.

5. AWARD OF CONTRACT:

Bidder having scored highest marks in Final evaluation as per para 4(c), will be awarded the contract. After acceptance of Technical and Financial bid, an Award Letter shall be issued, in duplicate, to the successful bidder, and the selected Firm, within 15 days of receipt of Award Letter, sign and return the duplicate copy of the Award Letter in acknowledgement thereof. In the event the duplicate copy of the Award Letter duly signed by the Firm is not received by the stipulated date, the Authority may, unless it consents to extension of time for submission thereof, cancel the Award Letter issued to it.

6. MAILING ADDRESS/ CONTACT INFORMATION:

The following address details can be used for any correspondence, queries clarification and communication purposes via email and/or telephone calls:

Address	National Cyber Emergency Response Team (nCERT) HQ's, L- Block, Pakistan Secretariat, Islamabad
Telephone	051-9203421-22
Email	bid@pkcert.gov.pk
Website	www.pkcert.gov.pk

Details of Items Lot-Wise

Lot	Item Description	Qty	Unit Price with GST	Total Price With GST
1 (MicroData Center Solution)	Compute Node	03		
	Firewall	01		
	Core Switch	01		
	Access Switch	02		
	Access Point	06		
	SAN Storage	01		
	Smart Rack	01		
2 (Red Team Suite)	Security Validation Platform (Indigenous Solution)	01		
	Advanced Security Validation Platform (Red & Purple Team) - (Indigenous Solution)	01		
	Offensive Security Toolkit	01		
	ClaudeMax Subscription license	03		
3 (End-User Compute)	Laptop	20		
	Wireless Mouse + Keyboard Combo	20		
	Portable SSD	02		
	Portable USB	10		
	Heavy Duty Color Printer	02		
4 (Video Wall Solution)	100-Inch LED / QLED Smart Television	02		

Technical Specifications

Lot 1. (MicroData Center Solution)		
ITEM NO. 01	Compute Node	03
S#	Technical Description, Specifications and Standards Required	
1.1	2U Chassis with min 12 (3.5") 2x (2.5") Disk Slots or better	
1.2	2x Enterprise-Grade Processors min 32 Cores/64 Threads or higher, Base frequency \geq 2.6 GHz (\geq 2.8 GHz preferred) ,Turbo frequency \geq 3.5 GHz. Must support: 64-bit architecture and Hardware virtualization (Intel VT-x / AMD-V) Cache memory \geq 24 MB per processor	
1.3	Min 256 GB RAM, Configuration 8*32GB DDR5 5600 MHZ or higher	
1.4	2x 480GB/960GB 2.5" SATA SSD (configured with RAID1) or better	
1.5	Minimum: 4 \times 10GE SFP+ ports (with multimode transceivers, 4 \times 1G RJ45 Ethernet ports	
1.6	Embedded remote management with web-based console (iDRAC/iLO or equivalent), supporting remote KVM, power control, and monitoring, with compatibility for VMware, Hyper-V, and KVM virtualization platforms.	
1.7	Raid Card 8GB cache with Raid(0,1,10,5,6) and Pass-through (JBOD) mode supported or better	
1.8	Dual hot-swappable redundant power supplies with high-efficiency rating (80 PLUS Platinum or better).	
1.9	Embedded Server Management Software for Remote Management	
1.10	Rack mounting rail kit , Front bezel (lockable preferred)	
1.11	OEM Backed Warranty (3 Years) with 24/7 technical support Next Business Day replacement (preferred)	

- i. **The bidder (who qualified) must assign a qualified onsite (Technical/Resident) engineer for 1-Years to perform the installation, integration, configuration, and commissioning of the Lot1 Micro Data Center solution.** The bidder shall also be responsible for supplying, installing, and properly terminating all required interconnection and power cabling associated with the infrastructure. This includes complete internal rack cabling as well as all necessary cabling between the rack and the laboratory area. All cabling shall be installed following industry best practices, ensuring proper routing, secure mounting, clear labeling, and compliant termination to guarantee reliable operation, ease of maintenance, and a well-organized installation environment.

ITEM NO. 02	Firewall	01
Technical Description, Specifications and Standards Required		
Must be a globally recognized enterprise-grade Next-Generation Firewall with proven threat intelligence and a strong presence in the Pakistan market for at least 5 years.		
Must Have OEM Presence in Pakistan For Minimum 5 Year		
Must Have Full Features Working Even License Is Expired		
Must Have Minimum 7 NGFW Throughput (FW + SA + IP		
Must Have Minimum 3.5 Threat Protection Throughput (FW + SA + IPS + Antivirus)		
Must Have Unrestricted Concurrent User		

Must Have Minimum 128GB Storage Capacity
Must Have Minimum 4 x 1G Ethernet Interfaces, & 2 >= 10G SFP+ Interfaces
Must Include Intrusion Prevention System (IPS), Anti-Virus & Anti-Malware, Email Security Protection, Cloud-Based Security Sandbox, Web Filtering, Application Control, Bandwidth Management
Must Quote Minimum 100 Concurrent Users for SSL VPN, Support for IPSec VPN and SSL VPN
Must Quote 3 Years Complete Security Features License
Must Quote 3 Years Software Upgrade & 24x7
Must Quote 3 Years Hardware Warranty Service
Must Quote Onsite Configuration & Installation
Must Quote Onsite Training (Mandatory)
Product Certification For 2 Participant (Optional) Extra Marks
The solution must continue to provide basic firewall functionality (L3/L4 filtering, routing, NAT) after license expiry. Advanced security features (IPS, AV, sandbox, etc.) may require valid subscription.”
The bidder must be an authorized partner/reseller/distributor of the OEM and must provide a valid authorization certificate.”

ITEM NO. 03	Core Switch	01																								
S#	Technical Description, Specifications and Standards Required																									
3.1	1 Interface Requirements 48 × 10G SFP+ ports ≥ 2 × 40G or 100G QSFP uplinks																									
3.2	1 Performance Requirements The switch must meet or higher specs: <table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Parameter</th> <th style="text-align: left;">Minimum Requirement</th> </tr> </thead> <tbody> <tr><td>Switching capacity</td><td>≥ 640 Gbps (up to 960 Gbps preferred)</td></tr> <tr><td>RAM</td><td>≥ 4 GB</td></tr> <tr><td>Flash</td><td>≥ 2 GB</td></tr> <tr><td>MAC address table</td><td>≥ 384K</td></tr> <tr><td>ARP entries</td><td>≥ 62K</td></tr> <tr><td>Ipv4 routing entries</td><td>≥ 250K</td></tr> <tr><td>Ipv6 routing entries</td><td>≥ 80K</td></tr> <tr><td>Jumbo frame</td><td>≥ 9K</td></tr> <tr><td>VLANs</td><td>≥ 4K</td></tr> <tr><td>VRF instances</td><td>≥ 1,000</td></tr> <tr><td>VRRP groups</td><td>≥ 255</td></tr> </tbody> </table>		Parameter	Minimum Requirement	Switching capacity	≥ 640 Gbps (up to 960 Gbps preferred)	RAM	≥ 4 GB	Flash	≥ 2 GB	MAC address table	≥ 384K	ARP entries	≥ 62K	Ipv4 routing entries	≥ 250K	Ipv6 routing entries	≥ 80K	Jumbo frame	≥ 9K	VLANs	≥ 4K	VRF instances	≥ 1,000	VRRP groups	≥ 255
Parameter	Minimum Requirement																									
Switching capacity	≥ 640 Gbps (up to 960 Gbps preferred)																									
RAM	≥ 4 GB																									
Flash	≥ 2 GB																									
MAC address table	≥ 384K																									
ARP entries	≥ 62K																									
Ipv4 routing entries	≥ 250K																									
Ipv6 routing entries	≥ 80K																									
Jumbo frame	≥ 9K																									
VLANs	≥ 4K																									
VRF instances	≥ 1,000																									
VRRP groups	≥ 255																									
3.3	<ul style="list-style-type: none"> • Layer-2 Features The switch must support: <ul style="list-style-type: none"> • 802.1Q VLANs, QinQ and Flexible QinQ • Private VLANs and Guest VLAN • GVRP and VLAN isolation • LACP with ≥ 64 groups • MSTP, RSTP, STP • Ethernet Ring Protection Switching (G.8032) 																									

	<ul style="list-style-type: none"> • Loop detection and fault detection features
3.4	<ul style="list-style-type: none"> • Layer-3 Routing Requirements <p>The switch must support:</p> <ul style="list-style-type: none"> • 4.1 Ipv4/Ipv6 Dual Stack • Wire-speed forwarding for Ipv4 and Ipv6 • Static routing (Ipv4 & Ipv6) • RIP/RIPng • OSPFv2 / OSPFv3 • BGP / BGP+ • IS-IS / IS-Isv6 • Policy-Based Routing • VRRP / VRRPv3 • ECMP routing
3.5	<ul style="list-style-type: none"> • Network Virtualization & SDN <p>The proposed solution must support:</p> <ul style="list-style-type: none"> • 6.1 VxLAN / EVPN • L2/L3 VxLAN Gateway • Ipv4 & Ipv6 VxLAN tunnels • BGP-EVPN • Distributed and centralized VxLAN gateway • End-to-End VxLAN DCI support
3.6	<ul style="list-style-type: none"> • QoS Requirements <p>The switch must support advanced QoS including:</p> <ul style="list-style-type: none"> • 8 hardware queues per port • Scheduling algorithms: SP, RR, WRR, WDRR, SP+WRR, SP+WDRR • Traffic shaping and rate limiting • DSCP / CoS / 802.1p classification • RED/WRED congestion management
3.7	<ul style="list-style-type: none"> • Security Requirements <p>The switch must provide enterprise security including:</p> <ul style="list-style-type: none"> • Access Security • 802.1X authentication • Port security • MAC + IP + VLAN binding • DHCP Snooping / ND Snooping • IP Source Guard • Threat Protection • Dynamic ARP Inspection • DoS/DdoS protection • Storm control • ARP guard & ARP suppression • AAA • RADIUS • TACACS+ • Portal authentication
3.8	<ul style="list-style-type: none"> • Monitoring & Management <p>The switch must support:</p> <ul style="list-style-type: none"> • SNMP v1/v2/v3 • RMON • SYSLOG • Telemetry & sFlow • SPAN / RSPAN / ERSPAN

	<ul style="list-style-type: none"> • LLDP and IP-SLA • Web GUI, CLI, Telnet, SSH • TR-069 management • Zero Touch Provisioning via DHCP or USB
3.9	<p>The solution must include:</p> <ul style="list-style-type: none"> • All features enabled without additional license tiers • Free firmware upgrades and updates • No recurring feature licensing costs
4.0	<ul style="list-style-type: none"> • Warranty & Support • Minimum 3-year OEM warranty • Onsite installation and commissioning required

Access Switches		
ITEM NO.	Access Switch 1G	02
04		
S#	Technical Description, Specifications and Standards Required	
4.1	<p>The switch must provide:</p> <ul style="list-style-type: none"> • Minimum 24 × 10/100/1000 Mbps RJ-45 Ethernet ports • Minimum 4 × 10Gb SFP+ uplink ports • Dedicated RJ-45 Console Port • USB 2.0 management port • Non-blocking switching architecture 	
4.2	<p>Switching performance must meet or exceed:</p> <ul style="list-style-type: none"> • Switching Capacity: ≥128 Gbps • MAC Address Table: ≥16K entries • Jumbo Frame Support: ≥12 KB 	
4.3	<ul style="list-style-type: none"> • PoE Requirements <p>Switch must support enterprise PoE features:</p> <ul style="list-style-type: none"> • PoE Standard: IEEE 802.3af / 802.3at • Minimum PoE Budget: ≥380 Watts • Per-port power management and monitoring • Power scheduling and consumption control 	
4.4	<p>Layer-2 Features</p> <p>Switch must support enterprise L2 switching including:</p> <p>VLAN Capabilities</p> <ul style="list-style-type: none"> • IEEE 802.1Q VLAN tagging • VLAN capacity: ≥4K VLANs • Private VLAN • Guest VLAN • Voice VLAN • Protocol VLAN / Subnet VLAN • QinQ & Flexible QinQ • GVRP support <ul style="list-style-type: none"> • Spanning Tree & Loop Prevention • STP / RSTP / MSTP • BPDU Guard, Root Guard, Loop Guard • Loopback detection • Storm control and flood control 	

	<p>Link Aggregation</p> <ul style="list-style-type: none"> • IEEE 802.3ad LACP • ≥64 LACP groups • ≥8 ports per aggregation group
4.5	<p>Layer-3 Features</p> <p>The switch must support Layer-3 Lite routing:</p> <ul style="list-style-type: none"> • Static Ipv4 and Ipv6 routing • ARP / ICMP / DNS / NTP • DHCP Client support (Ipv4 & Ipv6)
4.6	<p>Multicast Support</p> <p>Must support:</p> <ul style="list-style-type: none"> • IGMP v1/v2/v3 Snooping • IGMP Proxy • MLD Snooping • Multicast VLAN Registration (MVR)
4.7	<p>Security Features</p> <p>Access Control & Authentication</p> <p>Switch must support:</p> <ul style="list-style-type: none"> • 802.1X authentication • MAC + IP + VLAN binding • AAA, RADIUS, TACACS+ • Portal authentication <p>Network Protection</p> <ul style="list-style-type: none"> • DHCP Snooping • Dynamic ARP Inspection • IP Source Guard • ND Snooping • Host Guard • DoS/DdoS attack protection • ARP attack mitigation • Port Security & ACLs <ul style="list-style-type: none"> • 7.3 Access Control Lists • Ipv4 / Ipv6 ACL • MAC ACL • Time-based ACLs
4.8	<p>High Availability & Resilience</p> <p>Switch must support:</p> <ul style="list-style-type: none"> • Ethernet Ring Protection (G.8032) with ≤50ms failover • ULFD / UDLD • BFD with static routing • CPU protection mechanisms
4.9	<p>Management & Monitoring</p> <p>Must support multiple management methods:</p> <ul style="list-style-type: none"> • CLI, Web GUI (HTTP/HTTPS) • SNMP v1/v2/v3

	<ul style="list-style-type: none"> • SYSLOG & RMON • sFlow / Telemetry • LLDP • Firmware upgrades without additional license cost
5.0	Standards Compliance Switch must comply with IEEE standards including: <ul style="list-style-type: none"> • 802.3, 802.3ab, 802.3ae (10G) • 802.1Q VLAN • 802.1X NAC • 802.1p QoS • 802.1d/w/s STP family • 802.3ad LACP
5.1	<ul style="list-style-type: none"> • Warranty & Support • Minimum 3-year OEM warranty • Onsite installation and commissioning required

Wireless Access Points		
ITEM NO.	Access Point	06
05		
S#	Technical Description, Specifications and Standards Required	
1.1	Access Point must support 802.11 abgn/ac/ax standards	
1.2	Support MU-MIMO and OFDMA	
1.3	The access point should work on 2.4GHz and 5 GHz band simultaneously.	
1.4	Access Point should support 574 Mbps (2.4 GHz) and 1200 Mbps (5 GHz).	
1.5	Access point must work on 2 x 2 MU-MIMO with 2 Spatial Streams on both 2.4 and 5 GHz band. (Controller High Priority)	
1.6	Access Point should support Channelization of 20 MHz, 40 MHz and 80 MHz.	
1.7	Support multiple Integrated dual polarized smart antennas with PD-MRC.	
1.8	BeamFlex+ Antennas: Extended coverage and optimized throughput with patented multidirectional antennas and radio patterns	
1.9	Hardware must have a physical gain of 3dBi on both 2.4GHz and 5GHz antennas, with an additional chip-based gain of 4dB.	
2.0	Device must transmit Power upto 23dBm on both bands	
2.1	Access Point must be able to use all RF channel (not only non-overlapping channels) and maintain channel history with respect to Channel interference and throughput.	
2.2	AP must have one Gigabit PoE Ethernet port with 1 USB port support	
2.3	AP should support 802.3af POE standards.	
2.4	Wireless Security: WPA-PSK, WPA-TKIP, WPA2 AES, WPA3, 802.11i, Dynamic PSK.	
2.5	Implement Wi-Fi alliance standards WMM, Power Save, Tx Beamforming, LDPC, STBC, 802.11r/k/v	
2.6	The access point should support 802.1q VLAN tagging	
2.7	Should support rate limit and MAC base access control.	
2.8	Up to 200 or above Concurrent clients support.*/	
2.9	1 Year support must be included, support includes Advanced Hardware Replacement (Next Business Day) and Software upgrades.	

3.0	Proposed product must in the Wired and Wireless LAN infrastructure of Gartner Magic Quadrant for last 3 years.
3.1	Proposed brand must be Wi-Fi Alliance Certified
3.2	Proposed Access Point must be from a Tier-1, globally recognized enterprise networking vendor with a proven track record.

Storage Specifications		QTY 1
Item # 06	Requirements	Specifications
1	Storage Architecture	The proposed solution must be an enterprise-grade SAN storage system with active-active dual controllers, scalable to additional controllers or expansion shelves.
2	Controllers	Minimum dual active-active controllers with independent processing, seamless failover, and full redundancy to eliminate any single point of failure
3	Controller Cache	Each controller must have at least 64GB cache. The cache must be protected using battery backup or flash backup to prevent data loss. Performance cache must be separate from SSD tiering systems if tiering is used.
4	Processor Requirements	Each controller must have Enterprise-grade processor (Intel or equivalent) , Minimum 20 cores per controller
5	Disk Support	The storage should support SAS SSD, and NL-SAS disks
6	Front End Connectivity	Minimum: 4 × 10GE SFP+ ports per controller (or equivalent bandwidth) All ports must be: Fully populated with transceivers
7	Back End Connectivity	The storage system should support high-speed backend connectivity optimized for low latency and high throughput. Technologies such as SAS, NVMe, or equivalent are acceptable.”
8	Scalability	Must support: ≥ 1000 disk drives (scalable architecture) Expansion must be: Non-disruptive
9	Raid Support	Must support: RAID 5 RAID 6 RAID 10 or better
10	Storage Capacity	Minimum: 50 TB usable capacity after RAID 6 Must be: Without reliance on deduplication or compression
11	Data Protection Features	Snapshots: Must support: Point-in-time snapshots

		Independent recovery (no snapshot corruption) Replication: Must support: Synchronous replication Asynchronous replication
12	Multiprotocol Support	The proposed array should support FC, iSCSI, NFS, CIFS, 16G FC, 32G FC, 10G/25G/40G iSCSI connectivity natively without additional hardware
13	Warranty	3 Years 9x5 Next Business Day (NBD) Onsite Support. (Baseline)

Smart Rack		
ITEM NO.	Smart Mini Data Center Solution	01
07		
Technical Description, Specifications and Standards Required		
<p>1. Overall Parameters</p> <p>1) The overall dimension of micro data center indoor unit is: 2 x 600mm(width) * 1100mm(depth) * 2000mm(height). 2) The power input is: 220V/1Phase/50Hz-60Hz. 3) The available space is at least 26U for One Rack. 4) The available power is 1 x 6kVA. • 5) The available cooling is 1 x 3.5kW.</p>		
<p>2. Cabinet System</p> <p>1) The loading capacity of the cabinet is 1500kg. 2) The size of each cabinet is 600mm(width) * 1100mm(depth) * 42U(height). 3) The color is RAL9005. 4) The cabinet system use 9 folded frame. 5) The cabinet is fully closed to protect equipment from dust and harsh environment. The front door of cabinet is reinforced glass type and adopts insulation material on the back side of it to keep good thermal effect. The rear door the cabinet is double open steel type. 5) The locking of cabinet is 3in1 Access Control. 6) The cabinet comes with wheels and level feet.</p>		
<p>3. Power System</p> <p>1) The UPS capacity is 6kVA Online UPS. 2) The UPS mounting type is rack mount, and height is 2U. 3) The UPS power input is 220V/1Ph/50Hz-60Hz. 4) The product includes a power management module. The power management module works as power distribution, protection, metering and management. It's built in with manual bypass for UPS system. Detail specification is referred to within the wiring diagram. Qty = 1 Nos 5) The PDU is basic type. The power output sockets are C13*12Pcs + C19*4Pcs. Qty = 2 6) The battery module is for 10 to 15 mins battery backup.</p>		
<p>4. Power System</p> <p>1) The UPS capacity is 6kVA Online UPS. 2) The UPS mounting type is rack mount, and height is 2U. 3) The UPS power input is 220V/1Ph/50Hz-60Hz.</p>		

<p>4) The product includes a power management module. The power management module works as power distribution, protection, metering and management. It's built in with manual bypass for UPS system. Detail specification is referred to within the wiring diagram. Qty = 1 Nos</p> <p>5) The PDU is basic type. The power output sockets are C13*12Pcs + C19*4Pcs. Qty = 2</p> <p>6) The battery module is for 10 to 15 mins battery backup.</p>
<p>5. Cooling System</p> <p>1) The cooling is packaged DX type, and total cooling capacity is 1 x 3.5kW.</p> <p>2) The cooling power input is 220V/1Ph/50Hz-60Hz.</p> <p>3) The cooling system indoor unit is Top mount packaged with evaporator and condenser.</p> <p>4) The evaporator fan is EC fan type. The condenser fan is EC fan type.</p> <p>5) The cooling unit shipped with refrigerant charged. The refrigerant is R410A.</p> <p>6) Emergency ventilation method is opening front door & rear door of cabinet during high temperature.</p>
<p>6. Monitoring System</p> <p>1) The display of monitoring system is 10" touch type.</p> <p>2) The monitoring is wall mounted on the front door no occupying IT space.</p> <p>3) The monitoring sensors include smoke, water leaking, door status for both racks.</p> <p>4) The management of UPS includes display of UPS working mode, UPS alarms, UPS input power parameters, UPS output power parameters.</p> <p>5) The management of cooling includes display of cooling working mode, cooling alarms, and setting of target temperature and humidity, control by return or discharge, and ON/OFF unit.</p> <p>6) Monitoring function supports calculation of power usage and calculation of system PUE.</p> <p>7) 8 Port KVM with 17-inch screen should also be included.</p>
<p>7. Fire Extinguishing/ Suppression System</p> <p>The fire system should be rack mount, and height is 3U.</p> <p>The extinguisher gas should be FM200</p> <p>The extinguishing trigger method is temperature/smoke sensing and automatic release of firefighting gas.</p>
<p>8. Certification and terms for rack</p> <p>Product should be CE Certified and complying to international standards.</p> <p>Must Quote Onsite Design, Configuration & Installation</p> <p>Must Provide OEM Manufacturer Authorization Letter</p> <p>The Returning Organization (RO) must not be blacklisted in the past by any Federal and/or Provincial Organization.</p> <p>OEM must have Presence/Representative in Pakistan</p> <p>Minimum 01 Year Manufacturer Hardware & Software Warranty.</p>

Lot 2. Red Team Suite		
ITEM NO. 01	Security Validation Platform (Indigenous Solution)	01
S#	Technical Description, Specifications and Standards Required	
1.1	The solution must be an indigenously developed / locally developed security validation platform with full ownership of intellectual property residing with the bidding entity. The solution must demonstrate local development, local R&D, and in-country engineering support capabilities.	
1.2	The solution must provide an automated security validation pipeline that includes Dynamic Application Security Testing (DAST), Breach & Attack Simulation (BAS), and continuous assessment capabilities. It must support scheduled and event-triggered validation with customizable profiles (Quick, Standard, Deep, Full) and enable re-testing and remediation verification with automated validation of fixes.	

1.3	The solution must include a comprehensive attack simulation engine with an up-to-date library of attack techniques mapped to industry frameworks such as MITRE ATT&CK. It must support attack path analysis and graph-based visualization to reveal chains of exploitable vulnerabilities leading to mission-critical systems. The solution should leverage AI-assisted vulnerability triage and classification.
1.4	The solution must provide a unified console with an intuitive dashboard for configuration, execution, monitoring, and reporting across all security testing modules. It must include interactive attack path visualization (network graph view) for real-time understanding of attack chains, pivoting opportunities, and security control effectiveness.
1.5	The solution must support customizable testing parameters including proxy configuration, scan scope definition, and authentication mechanisms (Bearer tokens, JWT, API keys, session cookies, custom headers). It must allow tailoring of testing workflows to suit specific environments and objectives.
1.6	The solution must support testing across multiple environments and technologies, including: web applications (dynamic analysis), REST APIs (OpenAPI/Swagger), GraphQL endpoints, internal and external network services, cloud environments (public, private, hybrid), operating systems, databases, and infrastructure components.
1.7	The solution must provide API-first design for powerful integrations with DevOps pipelines (CI/CD), vulnerability scanners, SIEM/SOC platforms, and enterprise security tools. It must support webhooks, CLI-based execution, and automated security gates for seamless integration into existing security workflows.
1.8	The solution must be capable of identifying and targeting internal systems for network security validation, exploiting vulnerabilities in networks, hosts, and devices. It must imitate attacker methods for access and data manipulation while providing security control validation to test the effectiveness of existing defenses (firewalls, EDR, WAF). Conduct web application tests via detailed crawling, pivoting to servers, databases, and backend networks to confirm exploitability.
1.9	The solution must offer one-step validation of results from a wide range of leading third-party vulnerability scanners and web application scanners commonly used in the industry. It must prioritize and validate infrastructure weaknesses post-scan using AI-based risk prioritization, confidence scoring, and duplicate detection.
1.10	Indigenous Solution Requirements: The bidding entity must demonstrate that the solution is developed and maintained locally with in-country engineering team, local technical support, and direct access to development team for customizations and feature enhancements. Source code escrow or local source code availability may be requested. The bidder shall provide details of local R&D facilities, development team size, and local support infrastructure.
1.11	The bidder shall provide relevant certifications and professional qualifications (e.g., OSCP, OSEP, or equivalent) for implementation and support personnel. The bidder shall quote accordingly for 02 users / licenses.

ITEM NO.	Advanced Security Validation Platform (Red & Purple Team) — Indigenous Solution	01
02		
S#	Technical Description, Specifications and Standards Required	
2.1	The solution must be an indigenously developed / locally developed offensive security platform with full intellectual property ownership residing with the bidding entity. The solution must be available as a cloud-delivered (SaaS) platform securely accessible through a web browser interface, with optional on-premises or hybrid deployment models for deployments within local data centers. It must provide comprehensive in-	

	platform documentation, operational guidance, and an intuitive interface to assist users in effectively deploying and managing the platform.
2.2	The solution must provide a comprehensive suite of security validation capabilities covering the entire cyber kill chain. It must support full-scale adversary simulation, from initial compromise through to data exfiltration, and enable both targeted testing as well as complete end-to-end red team exercises. The platform must include SOC/XDR validation capabilities to measure detection effectiveness, MTTD/MTTR, and readiness scoring.
2.3	The solution must include advanced evasion techniques designed to test the effectiveness of EDR, antivirus, and other security controls. It must provide payload obfuscation capabilities, incorporate proprietary evasion methods continuously updated through ongoing research and development, and support process injection and advanced weaponization techniques for control validation purposes.
2.4	The solution must support real-world attack simulation scenarios including macro-based exploitation, phishing campaign simulation, and intrusion scenarios. It must enable testing of business logic flaws, workflow bypass, and authorization issues across applications and APIs.
2.5	The solution must provide low-profile command-and-control (C2) capabilities for authorized testing scenarios, support system reconnaissance and network discovery, and enable user activity monitoring while maintaining stealthy persistence within the environment during authorized engagements.
2.6	The solution must provide real-time monitoring of defensive actions and alert red teams to blue team detection and response activities during engagements. It must enable purple team exercises by facilitating collaboration between offensive and defensive teams, with capabilities for true/false positive analysis, security coverage analysis, and control validation.
2.7	The solution must support integration with existing security infrastructure, including SIEM, SOAR, XDR platforms, and vulnerability management tools. It must enable vendor consolidation to support coordinated, multi-stage security validation engagements across the enterprise.
2.8	Indigenous Solution Requirements: The bidding entity must demonstrate that the solution is developed, maintained, and supported locally with in-country engineering and R&D team. The bidder must provide details of local development facilities, source code ownership, local technical support team, and capability for custom feature development based on organizational requirements. Preference shall be given to solutions with no dependency on foreign entities for core development, updates, or critical support functions.
2.9	The bidder shall provide relevant certifications and professional qualifications (e.g., OSCP, OSEP, or equivalent) for implementation and support personnel. The bidder shall quote accordingly for 02 users / licenses.
3.0	The bidder shall quote accordingly for 02 Users

ITEM NO. 03	Offensive Security Toolkit	01
S#	Technical Description, Specifications and Standards Required	
4.1	The solution must be a cloud-delivered offensive security platform that is securely accessible through a web browser interface. It must support the secure download of locally generated payloads and provide comprehensive in-portal documentation along with operational guidance to assist users in effectively deploying and managing the platform.	

4.2	The solution must provide a comprehensive suite of red teaming tools that cover the entire cyber kill chain. It must support full-scale adversary simulation, from initial compromise through to data exfiltration, and enable both targeted testing as well as complete end-to-end red team exercises.
4.3	The solution must include anti-forensic payload capabilities designed to evade EDR and antivirus solutions, provide advanced payload obfuscation techniques, and incorporate proprietary evasion methods that are continuously updated through ongoing research and development. It must also support process injection and other advanced weaponization techniques.
4.4	The solution must support macro-based Office exploitation and steganographic payload delivery using image-based payloads. It must also enable the simulation of real-world phishing campaigns and intrusion scenarios.
4.5	The solution must provide low-profile command-and-control implants and support system reconnaissance and network discovery capabilities. It must also enable user activity monitoring while maintaining stealthy persistence within the environment.
4.6	The solution must provide real-time monitoring of defensive actions and alert red teams to blue team detection and response activities during engagements.
	The solution must integrate with Cobalt Strike using Beacon Object Files (BOFs) and reflective DLL loading, and it must also integrate with the Core Impact automated penetration testing solution. Additionally, the solution must support integration with third-party red team tools and enable vendor consolidation to support coordinated, multi-stage engagements.
	The bidder shall quote accordingly for 02 Users

ITEM NO. 4	Claude Max Subscription Licenses (min Price not exceeding 100\$) for Yearly Basis	03
S#	Technical Description, Specifications and Standards Required	
4.1	<p>Core Capabilities:</p> <ul style="list-style-type: none"> • Access to advanced models (e.g., Claude Opus 4.6, Sonnet 4.5, Haiku 4.5) for superior reasoning, coding, and multimodal tasks. • Conversational AI for writing, editing, content creation, and complex problem-solving. • Code generation, visualization of data, and execution in supported environments (including Claude Code on web and terminal). <p>Analysis of text, images, and documents with extended context windows.</p>	
4.2	<p>Productivity Enhancements:</p> <ul style="list-style-type: none"> • Unlimited projects for organizing chats, documents, and workflows. • Integration with tools such as Google Workspace (email, calendar, docs) and connectors for remote management. • Extended thinking modes for handling complex, multi-step tasks. • Web search integration and desktop extensions for enhanced functionality. <p>Memory across conversations and priority access during high-traffic periods.</p>	
4.3	<p>Usage and Performance:</p> <ul style="list-style-type: none"> • 5x higher usage limits compared to Pro (e.g., average users can send approximately 900 messages or 200-800 Claude Code prompts every five hours). • Higher output limits across all tasks. • Early access to new features and models. • Support for advanced integrations (e.g., Claude in Excel). <p>Enhanced capacity for intensive workloads, such as extended use of Opus models (e.g., 24-40 hours weekly).</p>	

Lot 3. End User Compute		
ITEM NO. 1	Laptops	20
S#	Technical Description, Specifications and Standards Required	
1.1	Core™ 7 240H; 16GB DDR5; 512GB; RTX™ 5050 8GB; Win 11 16"; WUXGA OR Equivalent	
1.2	Wireless keyboard combo & Mouse The bidder shall supply a wireless keyboard (with integrated touchpad) and mouse combo operating on 2.4 GHz RF and/or Bluetooth with a minimum 10-meter range and USB nano receiver. The keyboard shall be full-size (minimum 104 keys), spill-resistant, and include a responsive multi-touch touchpad, while the mouse shall feature an optical sensor with at least 1000 DPI resolution. The product must be brand new, energy-efficient, and covered by a minimum one-year warranty.	20

ITEM NO. 2	Portable SSD	02
S#	Technical Description, Specifications and Standards Required	
6.1	Up to 800 MB/s Transfer Speed, 1TB Storage Capacity, Bus Powered, USB-C 3.2 Gen 2 Interface, 2-years warranty	

ITEM NO. 3	USB	10
S#	Technical Description, Specifications and Standards Required	
7.1	64GB, Speed2 USB 3.2 Gen 1 compliant, Min. 2-years warranty	

ITEM NO. 4	Heavy Duty Color Printer	02
S#	Technical Description, Specifications and Standards Required	
5.1	Print Speed (A4): 33ppm, Fax	

Lot 4. Video Wall Solution		
ITEM NO. 1	100-Inch LED / QLED Smart Television	02
Technical Description, Specifications and Standards Required		
<p>General Requirement: The bidder shall supply brand-new 100-inch LED/QLED Smart Television units suitable for training rooms, control rooms, classrooms, and presentation environments. The equipment must be from a reputable international manufacturer and must include all required accessories for installation and operation.</p> <p>The offered product must support 4K Ultra HD resolution, smart operating system functionality, high refresh-rate motion processing, and modern connectivity interfaces.</p>		
Specification	Requirement Value / Details	
Screen Size	Minimum 100 inches Diagonal	
Display Technology	LED / QLED panel	
Resolution	4K Ultra HD (3840 × 2160)	
Aspect Ratio	16:9	

Viewing Angle	Minimum 178° horizontal / vertical
Brightness	Minimum 400 nits
Color Depth	10-bit or equivalent
Color Gamut	Wide color gamut / Quantum Dot technology
Response Time	≤ 8 ms
Video & Motion Processing	The television must support: HDR10 / HDR10+ HLG HDR Dolby Vision (preferred) MEMC (Motion Estimation Motion Compensation) Minimum refresh rate 120 Hz 144 Hz MEMC motion smoothing (preferred) AI picture enhancement / upscaling technology
Video & Motion Processing	
<p>HDR10 / HDR10+ HLG HDR Dolby Vision (preferred) MEMC (Motion Estimation Motion Compensation) Minimum refresh rate 120 Hz 144 Hz MEMC motion smoothing (preferred) AI picture enhancement / upscaling technology</p>	
Smart TV Platform	
Operating System	Android TV / Google TV or equivalent
RAM	≥ 2GB
Internal Storage	≥ 16 GB
Voice Control	Built-in voice assistant / smart voice search
Applications	YouTube, Netflix, Prime Video, browser support
Screen Casting	Chromecast / Miracast / AirPlay equivalent
Audio System	
Speaker Output	Minimum 20W – 50W
Audio Technology	Dolby Atmos / Dolby Audio / DTS
Speaker Type	Integrated stereo or 2.1 audio system
Connectivity & Interfaces	
HDMI ports:	Min 3
USB ports	Min 2
Ethernet:	1 × RJ45 LAN
Wireless	Dual-Band Wifi
Bluetooth:	Version 5.0 or higher
Audio Output:	Optical / HDMI eARC
Screen Mirroring	Supported
Physical & Installation Requirements	
<ul style="list-style-type: none"> • Slim or bezel-less industrial design • VESA mounting support • Wall mount bracket or floor stand included • Power supply AC 100–240V, 50/60Hz • Suitable for continuous operation environments 	
Accessories	

The vendor must provide:

- Original remote control with voice function
- Wall mount bracket or stand
- Power cable
- HDMI cable
- User manual

Warranty & Support: • Minimum 1-year manufacturer warranty

Local service support within Pakistan

Vendor must provide installation and commissioning⁴

Replacement or repair within warranty period

Compliance

The equipment shall comply with internationally recognized standards such as:

- CE / FCC or equivalent
- Energy efficiency standards
- Electromagnetic compatibility (EMC)