TENDER NOTICE

No. EA/02-18-2025

RFP For Supply and Installation Services of Telecom Switches and Routers

1. Bids are invited from the potential Authorized sources for the Supply and Installation Services of Telecom Switches and Routers as per RFP Annexure. This bid Document is also available on the Etisalat website (www.etisalat.af/en/about-us/doing-business-with-us/tenders).

2. RFP Deadline is **05 May 2025 Afghanistan time**.

3. Bid received after the above deadline shall not be accepted.

4. Bidders can provide either a sealed Hardcopy of the Proposal or a Softcopy of the Proposal through email. A hard copy can be submitted to Etisalat's Main office, Reception Desk (Tender Box). The softcopy shall be submitted through email (ashalizi@etisalat.af) and cc: (Ihsanullah@etisalat.af and marked clearly with the **RFP name, and number.**

5. The bidder shall submit the proposal with separate (Technical and Commercial) parts. The commercial part must be password password-protected document for a softcopy of the proposal, and we will request the password once here the concerned committee opens bids (starts the bid's Commercial evaluation). The bids shall be first evaluated technically. Technical evaluation will be based on the conformity to required technical specifications and compliance matrix specified in the Bidding Documents. Only technically compliant bids that meet all the mandatory service-effecting requirements will be evaluated commercially.

==

6. Etisalat Afghanistan reserves the right to accept or reject any or all bids and to annul the bidding process at any time, without thereby incurring any liability to the affected bidder(s) or any obligations to inform the affected bidder(s) of the grounds for Etisalat Afghanistan action.

7. All correspondence on the subject may be addressed to Ahmad Shikib Shalizi, Assistant Manager of Procurement, and Etisalat Afghanistan. Email ashalizi@etisalat.af and Phone No. +93781 204 040.

Ihsanullah Zirak

Director Procurement and Supply Chain

Ihsan Plaza, Shar-e-Naw, Kabul, Etisalat

Afghanistan

E-mail: ihsanullah@etisalat.af

(RFP)

For

Supply and Installation Services of Telecom Switches and Routers

1. DEFINITIONS

In this document, the following terms and meanings shall be interpreted as indicated:

1.1 Terms.

"Acceptance Test(s) "means the test(s) specified in the Technical Specifications to be carried out to ascertain whether the Goods, Equipment, System, Material, Items or a specified part thereof is able to attain the Performance Level specified in the Technical Specifications in accordance with the provisions of the Contract.

"Acceptance Test Procedures" means test procedures specified in the technical specifications and/or by the supplier and approved by EA as it is or with modifications.

"Approved" or "approval" means approved in writing.

"BoQ " stands for Bill of Quantities of each job/work as mentioned in this contract and its annexes according to which the contractor shall supply equipment & services and subject to change by agreement of both parties.

"Bidding" means a formal procurement procedure under which sealed bids are invited, received, opened, examined and evaluated for the purpose of awarding a contract.

"Bid/Tender Document" means the Bid/Tender documents issued by EA for invitation of Bids/Offers along with subsequent amendments and clarifications.

"Competent Authority" means the staff or functionary authorized by EA to deal finally with the matter in issue.

"Completion Date" means the date by which the Contractor is required to complete the Contract.

"Country of Origin" means the countries and territories eligible under the rules elaborated in the "Instruction to Bidders ".

"Contract" means the Contract between Etisalat Afghanistan (EA) and the Contractor and comprising documents.

"Contractor" means the individual or firm(s) ultimately responsible for supplying all the Goods/Equipment/Systems/Material/Items on time and to cost under this contract to EA.

"Contractor's Representative" means the person nominated by the contractor and named as such in

the contract and approved by EA in the manner provided in the contract.

"Contract Documents" means the documents listed in Article (Contract Documents) of the Form of Contract (including any amendments thereto) or in any other article in this contract.

"Contract Price" means the price payable to the Contractor under the Contract for the full and proper performance of its contractual obligations.

"Day" means calendar day of the Gregorian calendar.

"Delivery charges" means local transportation, handling, insurance and other charges incidental to the delivery of Goods to their final destination.

"Effective Date" means the date the Contract shall take effect as mentioned in the Contract.

"Etisalat Afghanistan (EA)" means the company registered under the Laws of Islamic Emirate of Afghanistan and having office at Ihsan Plaza Charahi Shaheed Kabul in person or any person dully authorised by it for the specific purpose for the specific task within the Contract and notified to contractor in writing.

"Final Acceptance Certificate" means the certificate issued by EA after successful completion of warranty and removal of defects as intimated by EA.

"Force Majeure" means Acts of God, Government restrictions, financial hardships, war and hostilities, invasion, act of foreign enemies, rebellion, revolution, riot, industrial disputes, commotion, natural disasters and other similar risks that are outside of Contractor's and EA's control.

"Liquidated Damages" mean the monetary damages imposed upon the contractor and the money payable to EA by the contractor on account of late delivery of the whole or part of the Goods.

"**L.o.A**" means Letter of Award issued by EA to successful bidder with regard to the award of tender.

"Month" means calendar month of the Gregorian calendar.

"Offer" means the quotation/bid and all subsequent clarifications submitted by the Bidder and accepted by EA in response to and in relation with the Bid Documents.

"Origin" means the place where the Goods are mined, grown or produced from which the ancillary services are supplied. Goods are produced when, through manufacturing, processing or substantial and major assembling of components, a commercially recognized product results that is substantially

==

different in basic characteristics or in purpose or utility from its components.

"EA's Representative" shall mean the representative to be appointed by EA to act for and on behalf of EA with respect to this Contract.

"Supplier/Vendor" (used interchangeably) means the individual or firm ultimately responsible for supplying all the Goods on time and to cost under this Contract acting individually alone or as a "prime contractor" for a consortium.

"Supplier's Representative" means the person nominated by the Contractor and named as such in the Contract and approved by EA in the manner provided in the Contract.

2. INTRODUCTION TO WORK.

2.1 Bids are invited the Supply and Installation Services of Telecom Switches and Routers in accordance with the stated specifications of Etisalat Afghanistan as in RFP Annexures.

2.2 The award of the tender will be based on best technical and price wise lowest offer.

3. Validity of Offers

The Tenders must be valid for a minimum of 90 days from the Tender closing date, or as may be specified by the Purchaser in the Tender documents.

4. CURRENCY:

The prices quoted shall be in Afghani for local Companies and USD for International firms.

5. Payment Terms

5.1 Payment shall be made by bank transfer after receipt of the original Hardcopy of the invoice.

5.2 Advance payment shall not be made to the contractor.

5.3 EA shall make prompt payment, within thirty days of submission of an invoice/claim by the contractor, subject to the availability of prerequisite documents specified under the contract and adjustment of penalty (if any) on account of late delivery and/or defective Goods replacement after confirmation from the Project Director.

5.4 Payments are subject to the deduction of income tax at the prevalent rate from the relevant

===

invoices of the contractor and paid to the Tax Authorities, except those especially exempted by the authorities. EA will issue a certificate of deductions to the contractor to enable him to settle tax returns with the concerned authorities.

6. Price:

Payments against the entire contract will be made by EA based on the contractor's ability to meet payment milestones as defined in the Bid Documents in the following manner.

6.1 For Supply of Equipment (Hardware & Software);

5.1.1 EA will make payment equal to 50% of the amount of equipment on the arrival of Equipment at site of installation and certification by EA Project Director/Manager of their receipt in good condition.

5.5.1.2 Balance 50% of the amount of equipment will be paid on issuance of RFS for the complete system area in individual city.

6.2 For Installation, Testing, Commissioning and Professional Services (if available).

6.2.1 EA will make payment equal to 75% of amount of Services cost when equipment is offered for Acceptance Testing in individual city.

6.2.2 Balance 25% of the amount of Services cost will be made at the time of issuance of final PAC for complete system in individual city.

6.3 For System Support and Maintenance Services (if available).

5.3.1 EA will make payment on quarterly basis at end of each quarter, after support/service is delivered.

7. Penalty:

7.1 If the contractor fails to complete the said job on or before the Completion Date, the Contractor shall pay to the Purchaser as and by way of Penalty resulting from the delay, the aggregate sum of one percent (1%) of Total Contract price of the delayed services for each week and pro-rata for parts of week, for delay beyond the specified date, subject to a maximum of ten percent (10%) of the Total Contract Price of the service(s). In the event that delay is only in respect of small items which do not affect the effective utilization of the system, penalty shall be chargeable only on the value of such delayed items.

7.2 Any penalty chargeable to the Contractor shall be deducted from the invoice amounts submitted by the Contractor for payment, without prejudice to the Purchaser's rights.

===

8. Construction of Contract:

The Contract shall he deemed to have been concluded in the Islamic Emirate of Afghanistan and shall be governed by and construed in accordance with Islamic Emirate of Afghanistan Law.

9. Termination of the Contract

9.1 If during the course of the Contract, the Contractor shall be in breach of the Contract and the Purchaser shall so inform the Contractor by notice in writing, and should the breach continue for more than seven days (or such longer period as may be specified by the Purchaser) after such notice then the Purchaser may immediately terminate the Contract by notice in writing to the Contractor.

9.2 Upon termination of the Contract the Purchaser may at his option continue work either by himself or by sub-contracting to a third party. The Contractor shall if so required by the Purchaser within 14 days of the date of termination assign to the Purchaser without payment the benefit to any agreement for services and/or the execution of any work for the purposes of this Contract. In the event of the services/jobs being completed and ready for utilization by the Purchaser or a third party and the total cost incurred by the Purchaser in so completing the required services/jobs being greater than which would have been incurred had the Contract not been terminated then the Contractor shall pay such excess to the Purchaser.

9.3 Etisalat has the right to terminate this Contract without cause at any time by serving a 30-day prior written notice to the Contractor.

10. Local Taxes, Dues and Levies:

10.1 The Contractor shall be responsible for all government related taxes, dues and levies, including personal income tax, which may be payable in the Afghanistan or elsewhere.

10.2 Withholding tax (if applicable) shall be deducted on local portion only as per prevailing rates as notified Islamic Emirate of Afghanistan. The amount of withholding Tax(s) is 2% of all project cost for local/registered companies who have Afghanistan Government Official Work License and 7% for International/ nonregistered companies.

Annexure-A (Bill of Quantity)
Summary

S.No	Project	Items	Item description (Details)	Quantity	Unit Price $	Total Price $
1	EGRX & VOIP Router	4x EGRX & 2xVOIP Router	10x10G Auto sensing port with GE, 10 x 1GE fixed electrical port, 10 x 1GE fiber, with accessories	6		
2		Engineering service	Site survey, transportation, installation, cabling, commissioning, service swap	6		
3		Technical support services	Level 3 support services (for 3 Year)	6		
4		Training (SP Core Architectures)	Overseas IP Training for 4 personnel for 2 weeks	1		
5	IPRAN Access Router for Base stations	IPRAN Access Router	4x100G, 20x10G Auto sensing port with GE, 20x1G optic, 20x1G Electrical, with accessories	20		
6		Training (QoS Design for SP Networks)	Overseas IP Training for 2 personnel for 2 weeks	1		
7	Access Switches 48 & 24 Ports (POE)	Access switches 48 Ports (POE)	48 x 1GE Electrical ports, 4 x 10G Auto sensing with GE, with accessories	55		
8		Access Switches 24 Ports (POE)	24 x 1GE Electrical ports, 4 x 10G Auto sensing with GE, with accessories	30		
9		Training (Segment Routing (SR-MPLS / SRv6))	Overseas IP Training for 2 personnel for 2 weeks	1		

===

Details:

		EGRX & VOIP Router		
	No.	**Item Name**	**Specification**	**QTY**
	1	4x EGRX & 2xVOIP Router	10x10G Auto sensing port with GE, 10 x 1GE fixed electrical port, 10 x 1GE fiber, with accessories	6
	2	Engineering service	Site survey, transportation, installation, cabling, commissioning, service swap	6
	3	Technical support services	Technical support services (for 3 Year)	6
	4	Training	Overseas IP Training for 4 personal for 2 weeks	1
		EGRX & VOIP Router (Compliance table and specifications)		
	No	**Specifications**	**Requirement Details**	**Compliance**
Main requirement	1	Type	Modular	
	2	Chassis Switching capacity bidirect	>1 Tb	
	3	NAT functionality & license	IPv4 NAT - 1M sessions	
	4	Port requirement	10x10G Auto sensing port with GE, 10 x 1GE fixed electrical port, 10 x 1GE fiber	
	5	SFP requirement	10x10G (5xSM 40km, 5x MM) , 10x1G Elect 10x1G (5xSM 40km, 5x MM)	
	6	Service Slot QTY requirement	>8 Mini / 4 full slot	
	7	Capacity per slot	based on interface capacities	
	8	Routing table size	>2M	
	9	Supervisor/control plane	1+1	
	10	fan	1+1	
	11	power supply	1+1	
	12	Power supply input type	DC	
	13	Operating temperature	to be shared by bidder	
	14	Life cycle	>7 year	
	15	Hardware EOS Date	>5 year	
	16	Software EOS Date	to be shared by bidder	
	17	IPv4	• Support for static routing as well as dynamic routing protocols, such as OSPF, IS-IS, and BGP-4, **GRE Tunnel** • Line rate forwarding on all interfaces in complex routing environments	
	18	IPv6	• Should support Various IPv4-to-IPv6 transition technologies: manual tunnel, automatic tunnel, 6to4 tunnel, GRE tunnel, and ISATAP tunnel • IPv4 over IPv6 tunnel and IPv6 Provider Edge (6PE) • IPv6 static routes • GRE Tunnels • Dynamic routing protocols, such as BGP4+, OSPFv3, and IS-ISv6 • IPv6 neighbor discovery, PMTU discovery, TCP6, ping IPv6, tracer IPv6, socket IPv6, static IPv6 DNS, IPv6 DNS server, TFTP IPv6 client, and IPv6 policy-based routing • Internet Control Message Protocol Version 6 (ICMPv6) Management Information Base (MIB), User Datagram Protocol Version 6 (UDP6) MIB, TCP6 MIB, and IPv6 MIB	
	19	MPLS	• MPLS TE, P2MP TE/mLDP, and MPLS/BGP VPN, in compliance with RFC 2547 • Inter-AS VPN Option A, Option B, and Option C • Integration with Internet services • Martini and Kompella MPLS L2VPN • L2VPN techniques, such as VPLS and VLL • IP interworking over heterogeneous media • Multicast VPN • MPLS-TP • EVPN • Remote LFA	
	20	L2	• IEEE 802.1Q, IEEE 802.1p, IEEE 802.3ad, and IEEE 802.1ab • STP, RSTP, and MSTP • EVC • VXLAN	

21	Reliability	• IP/LDP/VPN/TE/VLL FRR and IP/TE auto rerouting • IGP/BGP/ multicast route convergence, VRRP, RRPP, and IP-Trunk load balancing and backup • Hardware-based BFD of 3.3 ms, MPLS/Ethernet OAM, Y.1731, and routing protocol/port/VLAN damping • PW redundancy, E-Trunk, E-APS, and E-STP • In-service patching for smooth software upgrade • Passive backplane design • Redundancy backup for key components, such as route processing modules, SFUs, and power modules to guard against single points of failure • Switching between components that hot-back up each other, graceful restart (GR), NSF, NSR • Hot swap of all components	
22	Security	• OS Cryptographic support (AES, 3DES , SHA, RSA) **Ipsec (using cryptography algorithm)** • **GRE Over IPSec and vice versa** • GTSM • URPF • DHCP snooping • ARP attack defense and DoS attack defense • MAC address limit and MAC-IP binding • Secure Shell (SSH) and SSH version 2 (SSHv2)	
23	QOS	• Well-designed QoS and advanced scheduling and congestion avoidance technologies • Accurate traffic policing and traffic shaping • Complex rule definition and fine-grained flow identification • MPLS QoS, ensuring QoS for MPLS VPN, VLL, and PWE3 services • QPPB • TE-tunnel-oriented QoS	
Note: The NEs shall, at a minimum, support the above-listed protocols but may also include additional features or equivalent protocols for enhanced functionality.			

IPRAN Access Router for Base stations			
No.	Item Name	Specification	QTY
1	IPRAN Access Router	4x100G, 20x10G Auto sensing port with GE, 20x1G optic, 20x1G Electrical, with accessories	20
2	Training	Overseas IP Training for 2 personal for 2 weeks	1

IPRAN Access Router for Base stations (Compliance table and specifications)				
	No	Specifications	Requirement Details	Compliance
Main requirement	1	Type	Modular	
	2	Switching capacity bidirectional	>1Tb	
	3	NAT functionality & license	N/A	
	4	Port requirement	4x100G, 20x10G Auto sensing port with GE , 24x1G Elec, 20x1G optic	
	5	SFP requirement	4x100G SM 40Km, 10x10G SM 40km, 10x10G SM 10km, 20x1G SM 10KM, 20x1G Electrical	
	6	Service Slot QTY requirement	>8 Mini / 4 full slot	
	7	Capacity per slot	based on interface capacities	
	8	Routing table size	>2M	
	9	Supervisor/control plane	1+1	
	10	fan	1+1	
	11	power supply	1+1	
	12	Power supply input type	DC	
	13	Operating temperature	Temp -40 to 65 C	
	14	Life cycle	>7 year	
	15	Hardware EOS Date	>5 year	
	16	Software EOS Date	to be shared by bidder	
Features	17	IPv4	• Support for static routing as well as dynamic routing protocols, such as RIP, OSPF, IS-IS, and BGP-4 • Line rate forwarding on all interfaces in complex routing environments	
	18	IPv6	• Should support Various IPv4-to-IPv6 transition technologies: manual tunnel, automatic tunnel, 6to4 tunnel, GRE tunnel, and ISATAP tunnel • IPv4 over IPv6 tunnel and IPv6 Provider Edge (6PE) • IPv6 static routes • Dynamic routing protocols, such as BGP4+, RIPng, OSPFv3, and IS-ISv6 • IPv6 neighbor discovery, PMTU discovery, TCP6, ping IPv6, tracer IPv6, socket IPv6, static IPv6 DNS, IPv6 DNS server, TFTP IPv6 client, and IPv6 policy-based routing • Internet Control Message Protocol Version 6 (ICMPv6) Management Information Base (MIB), User Datagram Protocol Version 6 (UDP6) MIB, TCP6 MIB, and IPv6 MIB	
	19	MPLS	• MPLS TE, P2MP TE/mLDP, and MPLS/BGP VPN, in compliance with RFC 2547 • Inter-AS VPN Option A, Option B, and Option C • Integration with Internet services • Martini and Kompella MPLS L2VPN • L2VPN techniques, such as VPLS and VLL • IP interworking over heterogeneous media • Multicast VPN • MPLS-TP • EVPN • Remote LFA	
	20	L2	• IEEE 802.1Q, IEEE 802.1p, IEEE 802.3ad, and IEEE 802.1ab • STP, RSTP, and MSTP • EVC • VXLAN	

Features				
	17	IPv4	• Support for static routing as well as dynamic routing protocols, such as RIP, OSPF, IS-IS, and BGP-4 • Line rate forwarding on all interfaces in complex routing environments	
	18	IPv6	• Should support Various IPv4-to-IPv6 transition technologies: manual tunnel, automatic tunnel, 6to4 tunnel, GRE tunnel, and ISATAP tunnel • IPv4 over IPv6 tunnel and IPv6 Provider Edge (6PE) • IPv6 static routes • Dynamic routing protocols, such as BGP4+, RIPng, OSPFv3, and IS-ISv6 • IPv6 neighbor discovery, PMTU discovery, TCP6, ping IPv6, tracer IPv6, socket IPv6, static IPv6 DNS, IPv6 DNS server, TFTP IPv6 client, and IPv6 policy-based routing • Internet Control Message Protocol Version 6 (ICMPv6) Management Information Base (MIB), User Datagram Protocol Version 6 (UDP6) MIB, TCP6 MIB, and IPv6 MIB	
	19	MPLS	• MPLS TE, P2MP TE/mLDP, and MPLS/BGP VPN, in compliance with RFC 2547 • Inter-AS VPN Option A, Option B, and Option C • Integration with Internet services • Martini and Kompella MPLS L2VPN • L2VPN techniques, such as VPLS and VLL • IP interworking over heterogeneous media • Multicast VPN • MPLS-TP • EVPN • Remote LFA	
	20	L2	• IEEE 802.1Q, IEEE 802.1p, IEEE 802.3ad, and IEEE 802.1ab • STP, RSTP, and MSTP • EVC • VXLAN	
	21	Reliability	• IP/LDP/VPN/TE/VLL FRR and IP/TE auto rerouting • IGP/BGP/ multicast route convergence, VRRP, RRPP, and IP-Trunk load balancing and backup • Hardware-based BFD of 3.3 ms, MPLS/Ethernet OAM, Y.1731, and routing protocol/port/VLAN damping • PW redundancy, E-Trunk, E-APS, and E-STP • In-service patching for smooth software upgrade • Passive backplane design • Redundancy backup for key components, such as route processing modules, SFUs, and power modules to guard against single points of failure • Switching between components that hot-back up each other, graceful restart (GR), NSF, NSR • Hot swap of all components	
	22	Security	• ACL-based packet filtering • URPF • GTSM • DHCP snooping • ARP attack defense and DoS attack defense • MAC address limit and MAC-IP binding • Secure Shell (SSH) and SSH version 2 (SSHv2)	
	23	QOS	• Well-designed HQoS and advanced scheduling and congestion avoidance technologies on each LPU • Accurate traffic policing and traffic shaping • Complex rule definition and fine-grained flow identification • MPLS HQoS, ensuring QoS for MPLS VPN, VLL, and PWE3 services • QPPB • TE-tunnel-oriented QoS	

Note: The NEs shall, at a minimum, support the above-listed protocols but may also include additional features or equivalent protocols for enhanced functionality.

Access Switches 48 & 24 Ports (POE)			
No.	**Item Name**	**Specification**	**QTY**
1	Access switches 48 Ports (POE)	48 x 1GE Electrical ports, 4 x 10G Auto sensing with GE, with accessories	55
2	Access Switches 24 Ports (POE)	24 x 1GE Electrical ports, 4 x 10G Auto sensing with GE, with accessories	30
3	Training	Overseas IP Training for 2 personal for 2 weeks	1

		Carrier Grade IGW Router (Compliance table and specifications)		
	No	**Specifications**	**Requirement Details**	**Compliance**
Main requirement	1	Type	Fixed port	
	2	Chassis Switching capacity bidirectional	>100 Gbps for 24 port , >200 Gbps for 48 port	
	3	Port requirement for 24 ports	24 x 1GE Electrical ports (POE), 4 x 10G Auto sensing with GE	
	4	Port requirement for 48 ports	48 x 1GE Electrical ports (POE), 4 x 10G Auto sensing with GE	
	5	SFP requirement	4 X 10G (2X SM 1GE, 2X 2GE MM) for both 24 port and 48 port	
	6	Supervisor/control plane	1+1	
	7	fan	1+1	
	8	power supply	1+1	
	9	Power supply input type	AC + DC	
	10	Operating temperature	to be shared by bidder	
	11	Life cycle	>7 year	
	12	Hardware EOS Date	>5 year	
	13	Software EOS Date	to be shared by bidder	
Features	14	IPv4	• Support for static routing as well as dynamic routing protocols, such as RIP, OSPF, IS-IS, and BGP-4 • Line rate forwarding on all interfaces in complex routing environments	
	15	IPv6	• Should support Various IPv4-to-IPv6 transition technologies: manual tunnel, automatic tunnel, 6to4 tunnel, GRE tunnel, and ISATAP tunnel • IPv4 over IPv6 tunnel and IPv6 Provider Edge (6PE) • IPv6 static routes • Dynamic routing protocols, such as BGP4+, RIPng, OSPFv3, and IS-ISv6 • IPv6 neighbor discovery, PMTU discovery, TCP6, ping IPv6, tracert IPv6, socket IPv6, static IPv6 DNS, IPv6 DNS server, TFTP IPv6 client, and IPv6 policy-based routing • Internet Control Message Protocol Version 6 (ICMPv6) Management Information Base (MIB), User Datagram Protocol Version 6 (UDP6) MIB, TCP6 MIB, and IPv6 MIB	
	16	L2	• IEEE 802.1Q, IEEE 802.1p, IEEE 802.3ad, and IEEE 802.1ab • STP, RSTP, and MSTP • EVC • VXLAN	
	17	Reliability	• VRRP, RRPP, and IP-Trunk load balancing and backup • Hardware-based BFD of 3.3 ms, MPLS/Ethernet OAM, Y.1731, and routing protocol/port/VLAN damping • PW redundancy, E-Trunk, E-APS, and E-STP • In-service patching for smooth software upgrade • Passive backplane design • Switching between components that hot-back up each other, graceful restart (GR),	
	18	Security	• Flexible to integrate with NAC system • URPF • GTSM • DHCP snooping • ARP attack defense and DoS attack defense • MAC address limit and MAC-IP binding • Secure Shell (SSH) and SSH version 2 (SSHv2)	
	Note: The NEs shall, at a minimum, support the above-listed protocols but may also include additional features or equivalent protocols for enhanced functionality.			

Annexure-B

Cybersecurity Requirements

General Security Requirements:

1. Vendor must ensure their operating systems are up to date and is not End of Life/End of Support.
2. Vendor must ensure proper patch management of their servers in alignment with EA IT and Cybersecurity policies.
3. Vendor must ensure a licensed and standard AV solution is installed in all of their operating systems.
4. Vendor must ensure full cooperation and coordination with EA Cybersecurity team whenever required.
5. Vendor must not install any application without proper coordination and agreement of EA SOC Team.
6. The use of insecure cryptographic algorithms and protocols are strictly prohibited and all integrations and system communication must be based on secure and strong cryptographic algorithms.
7. Vendor must ensure strong protection of EA data stored on vendor's cloud.
8. Vendor must align all of their services and configurations in accordance to EA Information Security policies and standards.
9. Vendor must use and install only licensed applications.
10. The installation and Integration of servers must be aligned with IT and Cybersecurity requirements.
11. Vendor must not use/install any application/service that is not required.
12. Vendor must communicate any software installation with EA Cybersecurity team in advance.
13. Vendor must align their changes according to EA Change Management Policy.
14. Vendor must ensure all their operating systems are fully patched with the latest OS/Software updates.

==

15. Vendor must not use any OS that is/will be End of Life / End of Support in less than 3 year.

16. Only secure and strong cryptographic algorithms are allowed to be used in the vendor platforms.

17. System must support Role Based Access Control, and Rule Based Access Control

18. System must provide Strong authentication and authorization mechanisms

19. System must be capable of advanced logging mechanisms to ensure user activities are logged for audit and security purposes and the log must include all of the following at minimum.

- Failed and successful logins
- Modification of security settings
- Privileged use or escalation of privileges
- System events
- Modification of system-level objects
- Session activity
- Account management activities including password changes, account creation, modification…
- Event logs must contain the following details:
- Date and time of activity
- Source and Destination IP for the related activity
- Identification of user performing activity
- Description of an attempted or completed activity.

20. The system must support live log retention of 1 Year and backup up to 3 years.

21. System must be capable of encrypting the log files to ensure user does not modify or change the logs.

22. System must provide cryptographic algorithms such as AES 128/256 Bit, SHA 256/384/512 bits.

23. System must be secure against well-known attacks including but not limited to SQL Injection, XSS, CSRF, SSRF, Code Execution and other attacks.

24. Vendor system's password configuration must be aligned with EA Information security policies.

25. System must support integration with LDAP, IAM "Identity and Access Management" and PAM "Privileged Access Management" Solutions.

26. System must support external log synchronization mechanisms to push logs to another system for analysis such as SIEM and centralized log server.

27. The database must support the encryption of admin user's information with algorithms such as PBKDF2 and SHA256/384/512 bits.

28. The database platforms "if any" must support the encryption of data in-transit and at rest.

Important Note:

Bidders, vendors, and any concerned party shall fill all the fields in the below table, any missing or non-compliant item may cause disqualifying the proposed system from the Etisalat Security side.

No.	Description	Compliance (YES/NO/NA)	Comments
1	**Etisalat Security Requirements**		
1.1	The Contractor/Supplier/vendor to sign Non-Disclosure Agreement (NDA) with Etisalat before finalizing RFx/contract/POC agreement as per Etisalat NDA process.		
1.2	Contractor/Supplier/vendor equipment's (e.g. Servers, PCs, etc.) that are connected to Etisalat network must be securely wiped before taking out of Etisalat premises.		
1.3	The proposed/contracted system shall pass Etisalat Security Audit (Vulnerability Assessment/Penetration Testing) before go-live/service acceptance by Etisalat. Contractor/Supplier/vendor shall provide SLA for fixing Security gaps based on severity.		
1.4	Contractor/Supplier/vendor shall fix all security issues identified and reported by ETISALAT and/or Third Party Contracted to do the testing, with no		

No.	Description	Compliance (YES/NO/NA)	Comments
	additional cost		
1.5	Contractor/Supplier/vendor confirms that its products/solution are tested for weaknesses via methods such as Vulnerability Assessment, penetration testing, red teaming exercises and scans that check for compliance against the baseline security standards or security best practices, before the new product or any of its releases is delivered to ETISALAT. The Contractor/Supplier/vendor shall provide evidence/report of the security assessment/audit of the proposed solution.		
2	**Security Architecture**		
2.1	The Contractor/Supplier/vendor shall ensure that proposed solution shall comply with the applicable IT and Telecom Security standards (such as Afg. NESA (SIA) IA V2, Afg. DESC (ISR), Afg. TRA, 3GPP, ETSI, ENISA, CSA, NIST, PCI, ISO, GDPR etc.) The Contractor/Supplier/vendor shall confirm the applicable standard.		
2.2	The proposed solution shall support the latest operating systems and application versions. Contractor/Supplier/vendor to ensure proposed solutions will run the latest stable software, operating system, and firmware.		
2.3	The solution shall be designed with multi-tier architecture, (Demilitarized Zone (DMZ), middleware, and private network). Any system accessible from the Internet shall be on the DMZ		

No.	Description	Compliance (YES/NO/NA)	Comments
	and access to internal sensitive data shall be secured through the middle tier application proxy.		
2.4	The proposed solution shall not impact or relax existing Etisalat security control or posture.		
2.5	The performance of the proposed system shall meet the business requirements without disabling or removing any existing security control		
2.6	The Contractor/Supplier/vendor shall provide only secure methods of communication such as HTTPS, SFTP, SCP, TLS1.3, IPSEC, SRTP, SSH v2, SNMPv3 between the proposed nodes. Non-secure protocols such as Telnet, HTTP and FTP shall not be used.		
3	**Password Security**		
3.1	All Operating Systems (e.g. Linux and Windows) shall be hardened according to well-known standards such as, but not limited to NIST, CIS security benchmark, and NSA.		
3.2	The proposed system includes password management module that supports the following features:		
3.3	Setting the minimum password length		
3.4	Password complexity, and not accepting blank passwords		
3.5	Maximum password age and password history		
3.6	Account lockout		
3.7	Enforce changing password after first login		
3.8	Prompt / notify for the old password on password changes		
3.9	The password shall be saved in hashed format (i.e. irreversible encryption)		

No.	Description	Compliance (YES/NO/NA)	Comments
3.10	Forgetting or resetting password function shall support using OTP or email for verification		
4	**Authentication**		
4.1	The proposed system shall not provide access without valid username and password.		
4.2	All user access to the proposed system shall support Privilege account Management (PAM) integration.		
4.3	For public web applications, the proposed system supports and uses CAPTCHA or OTP to prevent password dictionary attacks		
4.4	For mobile applications, the proposed system shall support and uses fingerprint authentication method		
4.5	The proposed system supports and uses secure authentication protocols, like Kerberos, LDAP-S, NTLM V2 and above, HTTPs (for web applications)		
4.6	The proposed system will not use insecure authentication protocols, like NTLM v1, HTTP (for web applications)		
4.7	The proposed system shall support session timeout settings		
4.8	The proposed solution shall support secure API architecture to integrate systems to exchange data where deemed necessary.		
5	**Authorization**		
5.1	The proposed solution shall support role-based access controls that includes access profiles or security matrix (i.e. Role Name VS. Access Permissions)		

No.	Description	Compliance (YES/NO/NA)	Comments
5.2	The proposed system supports role-based access permissions, i.e. Administrator, Operator, Viewer, User…		
6	**Software Security**		
6.1	The software development and testing will not run on the production systems, and will be running in an isolated environment		
6.2	The software source code will not include clear-text passwords		
6.3	The software code will not include insecure protocols, like FTP, telnet …etc.		
6.4	The software testing will not use live/production sensitive or PII data unless it's masked as Etisalat security policy		
6.5	The proposed system enforces input and output validation to prevent security attacks, like SQL Injection, Buffer Overflow…etc.		
6.6	For web portals, the proposed system includes all security controls to prevent/protect from OWASP Top 10 security attacks and risks		
6.7	For mobile application, the proposed system shall include security checks / controls to protect from mobile attacks, like SSL Pinning, Jailbreak, Anti-debug, Anti-hooking, and Advanced Obfuscation…		

No.	Description	Compliance (YES/NO/NA)	Comments
7	**Security Event Logging**		
7.1	Proposed systems shall support standard logging protocols such as CIFS/Syslog/CSV logs files		
7.2	The system shall generate and support audit logs that contain the following fields (as a minimum): a) Username b) Timestamp (Date & Time). c) Client IP Address d) Transaction ID & session information		
7.3	The proposed solution shall support the integration with Etisalat NTP for time synchronization and accurate logging.		
8	**Public Cloud Security**		
8.1	Etisalat customers' and staff personal data (PII: name, contacts, address, Emirates ID, Passport number, Nationality …) is encrypted at rest and in transit using a strong industry-standard encryption protocol		
8.2	The Public Cloud setup that stores PII information shall be hosted in the Afghanistan		
8.3	The Public Cloud setup is hosted in a dedicated tenant for Etisalat (i.e. not shared)		
8.4	The Public Cloud data Center shall not be moved to another country or location without prior coordination and approval from Etisalat		
8.5	All Etisalat data will be permanently erased from the Public Cloud on termination of the service or		

	support agreement		
8.6	The proposed Cloud system supports Etisalat Cloud Access Security Broker (such as Microsoft MCAS, Netskope CASB)		
9	**Virtualization and Container Security**		
9.1	If applicable, Bidder shall ensure the proposed virtualized infrastructure, service based and micro services architecture to support multi tenancy, zoning & micro-segmentation, security visibility, secure virtualization (sVirt), trusted image signing, virtual Firewalls, DoS protection, Trusted platform module (TPM), Hypervisor & Host OS security to secure data and resources.		
9.2	The proposed solution shall support integration with Etisalat/Leading Container Security Solution, where applicable, to scan the container images and ensure malware protection of CI/CD pipeline.		
9.3	Suppliers must inform EA Cybersecurity of any non-conformity with defined EA policies and processes that are agreed upon in advance to acquire a written approval from EA Cybersecurity Department or senior management as required otherwise Supplier will be responsible for all the potential losses		

===

23 of 25

The following Information must be submitted with offer.

Bidder Contact Details	
Bidder Name	
Bidder Address	
Bidder Email Address	
Bidder Phone Number	
Bidder Contact Person Name	
Bidder Contact Person Phone No	
Bidder Contact Person Email Address	
Bidder Registration License Number	
License Validity	
TIN Number /Tax Number	

=============== end of documents ===============