TENDER NOTICE

No. EA/02-41-2024

For Providing Penetration Testing Tool

1. Bids are invited from your esteemed Corporation for Providing Penetration Testing Tool in Afghanistan as per RFP Annexure. This bid Document is also available on the Etisalat website (www.etisalat.af, Tenders).

2. RFP Deadline is **26 November 2024 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 (kshinwari@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 kshinwari@etisalat.af and Phone No. +93781 2049 48.

Ihsanullah Zirak
Director Procurement and Supply Chain
Ihsan Plaza, Shar-e-Naw, Kabul, Etisalat Afghanistan
E-mail**:** ihsanullah@etisalat.af

(RFP)

For

Providing Penetration Testing for Etisalat Afghanistan

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.
“CIF” means “Cost Insurance Freight” as specified in INCOTERM 2010.

“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.

“D.D.P” means Delivered Duty Paid as defined in the Incoterms 2010 including the unloading responsibility of bidder/seller.

“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.

“Goods Receipt Certificate” means certificate issued by the consignee certifying receipt of Goods in good order and condition.

“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.

“Specifications” means the specifications, provided in the Contract and its annexure and in EA Tender Specifications and where the Contract is silent and in cases of conflicting specifications appearing in the documents, based on the latest version of ITU-T recommendations.

“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.

“Warranty Period” shall mean the period of 12 months or any extended period starting from the acceptance of the delivered Goods in good order and conditions at consignee’s certified by EA authorized representative (s).

2. INTRODUCTION TO WORK.

2.1 Bids are invited for Providing Penetration Testing Tool in accordance with Etisalat specifications and Annexures.

3. Bill of Quantity (BoQ)

As per Annexure –A

4. 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 Purchaser in the Tender documents.

5. Price and Payment Term

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

5.2 Advance payment shall be not 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 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 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.

5.5 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.

5.5.1 For Supply of Equipment (Hardware & Software);

5.5.1.1 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.

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

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

5.5.2.2 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.

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

5.5.3.1 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 The Contractor shall not have the right to terminate or abandon the Contract except for reasons of force majeure.
9.4 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

Technical Scope of Work (SoW)

Technical Scope of Work (SoW) for Penetration Testing Tools and PTaaS service Combined Requirements

1. Technical Scope of Work for Penetration Tools

1.1 Objective

The primary objective of this project is to procure and implement **penetration testing tools** that comprehensively cover at least the following scope:

- Web Applications Penetration Testing
- Infrastructure Penetration Testing
- Internal Penetration Testing
- External Penetration Testing
- API Penetration Testing
- Mobile Application Penetration Testing

Additionally, the tools will enhance the organization's security posture by identifying and addressing vulnerabilities across these critical assets.

This toolset will enable the IT Security Operation team to simulate real-world attacks and assess the robustness of systems against diverse and dynamic threats, ensuring compliance with regulatory frameworks and industry standards.

1.2 Scope of Work

This document outlines the technical requirements for selecting, procuring, deploying, and operationalizing a set of penetration testing tools that will be used to identify security vulnerabilities in Etisalat Afghanistan's IT environment.

1.3 Gathering and Assessment

- **Understanding IT Infrastructure**: Evaluate the telecom company’s IT landscape, which includes web applications, mobile apps, databases, network devices, endpoints (including IoT), and servers (on-premises and cloud-based). This involves identifying the key assets to be tested and the potential security risks associated with each.

- **Security and Compliance Standards**: The penetration testing tools must align with applicable regulatory requirements (e.g., GDPR, PCI DSS, HIPAA) and industry standards (e.g., OWASP, NIST, ISO 27001, GSMA security guidelines).

1.4 Penetration Testing Tool Requirements

The penetration testing tools must meet the following technical requirements:

1.5 Application Penetration Testing

- **Web Application Testing**:
    - Ability to test for common vulnerabilities, including but not limited to:
        - **SQL Injection**
        - **Cross-site Scripting (XSS)**
        - **Cross-site Request Forgery (CSRF)**
        - **Remote Code Execution**
        - **Insecure Direct Object Reference (IDOR)**
    - Support for **OWASP Top 10** vulnerabilities.
    - Testing capabilities for **telecom-specific applications** that may involve custom protocols and application logic.
    - **Mobile Application Penetration Testing**:
        - Support for Android and iOS mobile applications, testing for issues such as insecure storage, weak encryption, reverse engineering vulnerabilities, and improper API integration.
        - Testing for secure mobile payment systems, messaging apps, and customer account management portals.

1.6 Database Penetration Testing

- **Database Vulnerability Identification**
    - Support for testing major databases such as **Oracle, MySQL, PostgreSQL, MongoDB**, and **SQL Server**.
    - Ability to detect **misconfigurations, privilege escalation vulnerabilities, and SQL injection**.

  - Identifying database-specific flaws such as weak passwords, lack of encryption, and insecure database configurations.
  - Evaluation of **telecom billing systems, call record databases**, and customer data management systems to detect data exposure risks.

1.7 Network Penetration Testing

- **Network Device Testing**:
  - Support for testing **routers, switches, firewalls, VPN gateways**, and **telecom-specific network components** (e.g., SS7, Diameter protocol devices).
  - Ability to detect vulnerabilities in **SS7**, **SIP**, and **Diameter** signaling protocols, commonly targeted in telecom attacks.
  - Testing for vulnerabilities such as **weak access controls, open ports, protocol manipulation, DDoS weaknesses, and routing attacks**.
  - **Internal and External Network Testing**: Simulation of both external attacks (from the internet) and internal network attacks (within the corporate network) to assess perimeter security and internal segmentation.

1.8 Endpoint Penetration Testing

- **Endpoint Security Assessment**:
  - Ability to test **workstations, laptops, IoT devices**, and **telecom-specific hardware** (e.g., mobile base stations, telecom switches) for vulnerabilities.
  - Detect insecure configurations, unpatched software, **malware vulnerabilities**, and **privilege escalation issues**.
  - Ensure tools can test different operating systems including **Windows, macOS, Linux**, and **Android**.
  - Identify **IoT** vulnerabilities specific to the telecom industry, such as insecure APIs, weak authentication, and open communication channels.

1.9 Server Penetration Testing

- **Operating System Security**:
  - Test for vulnerabilities in various server operating systems, including **Windows Server, Linux**, **Unix**, and **AIX** etc.
  - Identification of common vulnerabilities such as **unpatched exploits**, **insecure file permissions**, **weak services**, and **privilege escalation paths**.

- Cloud environment compatibility with support for testing servers hosted in **AWS, Azure, and Google Cloud** environments.
- Testing for **telecom-specific services**, such as call processing and billing systems hosted on servers.

1.10 Cloud and Container Penetration Testing

- **Cloud Infrastructure Testing**:
  - Penetration testing tools must be compatible with cloud infrastructure, able to identify vulnerabilities in **Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS)**, and **Software-as-a-Service (SaaS)** environments.
  - Detecting misconfigurations in **cloud storage**, **virtual machines**, and **cloud networking**.
  - Container and microservices support (e.g., Docker, Kubernetes), testing for vulnerabilities like **insecure container images, runtime exploitation**, and **inadequate isolation**.

1.11 Automation, Reporting, and Integration Capabilities

1.12 Automation and Continuous Testing

- **Automated Scans**: Tools must support automated, scheduled scans for regular testing across the entire environment, including the ability to simulate advanced persistent threats (APTs) and zero-day vulnerabilities.
- **Integration with CI/CD**: The tools should integrate with the organization's existing DevOps and CI/CD pipelines (e.g., Jenkins, GitLab, or GitHub Actions) to allow continuous security testing as part of the development and deployment process.

1.13 Customizable Attack Simulations

- **Advanced Exploit Testing**: The tool should support **customizable attack simulations**, enabling users to create specific attack scenarios relevant to the telecom sector (e.g., simulating DDoS attacks, SS7 vulnerabilities, and telecom fraud).
- **Post-exploitation Capabilities**: Ability to explore **post-exploitation scenarios**, simulating what attackers could achieve after gaining initial access, such as lateral movement, privilege escalation, and data exfiltration.

1.14 Comprehensive Reporting and Risk Assessment

- **Detailed Reports**: Tools must provide detailed reports, including risk assessments, vulnerability descriptions, and actionable remediation steps.
- **Executive-level Summaries**: Generate high-level reports for non-technical stakeholders, summarizing key findings and business risks, and aligning them with regulatory and compliance requirements.
- **Custom Reporting**: Support for customized reporting templates that align with specific compliance frameworks (e.g., PCI DSS, GDPR, NIST) and telecom regulations (e.g., GSMA security guidelines).

1.15 Usability, Training, and Support

1.16 Ease of Use

- **User-friendly Interface**: The tools should have an intuitive interface, enabling cybersecurity personnel to conduct tests efficiently, with minimal training.
- **Skill Levels**: The tools should cater to both entry-level and advanced cybersecurity professionals by offering different modes (e.g., guided testing for junior staff, advanced manual testing for senior analysts).

1.17 Training and Onboarding

- **Comprehensive Training Program**: Vendor must provide initial training and onboarding sessions to ensure that the cybersecurity team can effectively use the penetration testing tools.
- **Ongoing Training and Updates**: Continuous access to training materials, product updates, and knowledge bases is essential for maintaining proficiency as new vulnerabilities emerge.

1.18 Support and Maintenance

- **24/7 Technical Support**: Vendor should offer 24/7 support for troubleshooting issues related to tool usage, configuration, or integration.
- **Product Updates**: Tools must be regularly updated with new exploits, vulnerability databases, and scanning algorithms to stay relevant against emerging threats.

1.19 Deliverables

The vendor must provide the following:

- **Penetration Testing Toolset**: A comprehensive suite of tools capable of addressing the requirements for application, database, network, endpoint, and server testing.
- **Implementation Plan**: A detailed plan for integrating the toolset into the existing IT infrastructure.
- **Testing and Validation**: Conduct tests in a controlled environment to validate tool accuracy and effectiveness.
- **Documentation**: Detailed user manuals, administrator guides, and technical documentation for integration.
- **Training**: Initial training sessions for all relevant stakeholders, followed by ongoing support and access to resources.
- **Support and Maintenance**: Ongoing product support, regular updates, and access to a knowledge base.

2. Scope of Work Document for Penetration Testing as a Service (PTaaS)

2.1 Introduction

This Scope of Work (SoW) document outlines the deliverables, activities, and objectives for Penetration Testing as a Service (PTaaS) to be provided to Etisalat Afghanistan EA. The purpose of this PTaaS engagement is to identify and mitigate security vulnerabilities across critical assets including web applications, APIs, mobile applications, and network infrastructure, both internal and external.

2.2 Objectives

The PTaaS will focus on identifying vulnerabilities that could potentially lead to unauthorized access, data breaches, or disruption of services. This engagement aims to:

- Enhance overall security posture through a proactive approach.
- Identify vulnerabilities and provide actionable recommendations.
- Comply with industry regulations and standards (e.g., PCI DSS, ISO 27001).
- Safeguard sensitive customer data and proprietary information.

2.3 Scope of Penetration Testing Services

The PTaaS will encompass the following testing types:

2.4 Web Application Penetration Testing

- **Objective:** To identify vulnerabilities in web applications that may allow unauthorized access, data leakage, or service interruption.
- **Scope:** Includes all customer-facing and internal web applications defined by Etisalat Afghanistan.
- **Testing Areas:** Authentication and authorization mechanisms, input validation, session management, data encryption, and security misconfigurations.
- **Methodology:** OWASP Top Ten, SANS CWE Top 25, and any custom threats identified by Etisalat Afghanistan.

2.5 Infrastructure Penetration Testing

- **Objective:** To assess the security of the organization's internal and external network infrastructure.
- **Scope:** Includes servers, routers, firewalls, switches, network devices, and operating systems.
- **Testing Areas:** Network configuration, access controls, open ports, known vulnerabilities in systems, and unauthorized access points.
- **Methodology:** NIST SP 800-115, CREST standards, and Etisalat Afghanistan-specific threat scenarios.

2.6 Internal Penetration Testing

- **Objective:** To evaluate the security of systems and services from within the internal network.
- **Scope:** Includes user workstations, privileged accounts, servers, and critical systems accessible within the company's local area network.
- **Testing Areas:** Privilege escalation, lateral movement, sensitive data exposure, and unauthorized access controls.
- **Methodology:** Simulated insider threat scenarios and targeted exploitation of internal services.

2.7 External Penetration Testing

- **Objective:** To simulate attacks originating from the external environment.
- **Scope:** Includes all internet-facing assets such as websites, email servers, DNS servers, and publicly exposed APIs.
- **Testing Areas:** Perimeter defenses, brute force and password attacks, vulnerability in exposed services, and potential access to internal systems.
- **Methodology:** Reconnaissance, vulnerability scanning, targeted exploitation, and analysis of publicly accessible interfaces.

2.8 API Penetration Testing

- **Objective:** To assess the security of APIs used for data exchange between applications, third-party integrations, and mobile applications.
- **Scope:** Includes all RESTful, SOAP, and GraphQL APIs exposed externally and internally.
- **Testing Areas:** Authentication, authorization, input validation, data validation, and session management in APIs.

- **Methodology:** OWASP API Security Top 10, custom threat models, and Etisalat Afghanistan-specific use cases.

2.9 Mobile Application Penetration Testing

- **Objective:** To test mobile applications for security vulnerabilities that may compromise customer or business data.
- **Scope:** Includes Android and iOS applications, backend servers, and third-party integrations used within mobile applications.
- **Testing Areas:** Local data storage, encryption, API calls, authentication mechanisms, and sensitive data leakage.
- **Methodology:** OWASP Mobile Security Testing Guide (MSTG), OWASP Mobile Top Ten, and any organization-specific risks identified.

2.10 Roles and Responsibilities

- **Service Provider:** Conduct the penetration tests, deliver reports, and provide remediation guidance. Responsible for maintaining confidentiality and using testing toolsthat do not cause disruption to business operations.
- **Etisalat Afghanistan (Client):** Provide access to assets, clarify scope and objectives, coordinate with internal teams, and review testing reports.

2.11 Deliverables

The service provider will deliver the following:

1. **Pre-Engagement Report**: An initial assessment and outline of the test plan and schedule.
2. **Weekly Status Updates**: Updates regarding the testing progress, challenges, and preliminary findings.
3. **Final Report**: Detailed documentation of findings, including risk rating, impacted systems, and remediation recommendations.
4. **Remediation Support**: Assistance with understanding and implementing remediation steps.
5. **Retesting Report** (if applicable): Validation of fixes applied to previous vulnerabilities to ensure effective remediation.

2.12 Methodology and Standards

Testing will adhere to the following frameworks and guidelines:

- **OWASP**: For web applications, APIs, and mobile applications.
- **NIST**: General guidelines for infrastructure and network testing.
- **CREST**: For standardized approach in infrastructure and network testing.
- **Custom Threat Models**: Tailored to address specific threats pertinent to telecom systemsand infrastructure.

2.13 Confidentiality and Compliance

The provider will comply with Etisalat Afghanistan’s confidentiality requirements and any relevant regulations. All findings and data must be handled as confidential information.

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 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		

No.	Description	Compliance (YES/NO/NA)	Comments
	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 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)		
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		

No.	Description	Compliance (YES/NO/NA)	Comments
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		

RFP General Terms Compliance to be filled by Bidder.

S/N	Clause No. and General Terms	Comply (Yes/No)	Remarks
1	**4. VALIDITY OF OFFERS:**		
2	**6. ACCEPTANCE OF OFFERS:**		
3	**7. REGISTRATION/LEGAL DOCUMENTS OF THE BIDDER**		
4	**8. PAYMENTS**		
5	**9. PENALTY:**		
6	**10. CONSTRUCTION OF CONTRACT:**		
7	**11. TERMINATION OF THE CONTRACT BY THE PURCHASER**		
8	**12. LOCAL TAXES, DUES AND LEVIES:**		

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 ================