TENDER NOTICE

No. EA/02-22-2025

For Security Operations (SecOps) Solution

1. Bids are invited from your authorized partner for provisioning of Security Operations (SecOps) as per RFP Annexure. This bid Document is also available on the Etisalat website (www.etisalat.af, Tenders).

2. RFP Deadline is **16 June 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 (snabizada@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 snabizada@etisalat.af and Phone No. +93781204113.

==

Ihsanullah Zirak

Director Procurement and Supply Chain

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

Afghanistan

E-mail**:** ihsanullah@etisalat.af

(RFP)

For

Security Operations (SecOps) Solution

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 provisioning of Security Operations (SecOps) Solutions in accordance with Etisalat specifications and Annexures.

3. Bill of Quantity (BoQ) and Scope of Work

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 EA shall make the payment on monthly basis.

6. 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.

7. Termination of the Contract:

7.1 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.

7.2 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.

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

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

8. Local Taxes, Dues and Levies:

8.1 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.

8.2 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 (BOQ) and Scope of Work:

1.0 Introduction:

Etisalat Afghanistan is seeking Security Operations and Incident Response services as part of its strategic initiative to establish strong proactive measures for detecting and responding to security incidents, cyber threats, and risks across its diverse IT and telecom environments. Vendors are invited to present their service offerings, including capabilities for real-time monitoring, log analysis, proactive anomaly detection, and security incident response. Additionally, vendors should demonstrate commitment to continual improvement in log correlation and alerting mechanisms to enhance overall security effectiveness.

2.0 Objective:

The primary objectives of the SecOps and Incident Response services are:

- 24/7 real-time security event monitoring, analysis, and threat detection.
- Vendor must have an expert incident response team with certified professionals(e.g, CISSP, CISM, CEH, GCIA, GCIH, or SOC analyst certifications) capable of performing root cause analysis and recommending appropriate controls to prevent security incidents.
  For more details, please refer to Section 3.2 – Incident Response Table.
- At least 5 years of proven experience in delivering SecOps services for telecom or similar sectors.

- A summary of at least two reference projects(preferably in telecom or similar sectors).
- Immediate response to security incidents to contain, eradicate, and remediate threats.
- Integration and correlation of alerts across all security platforms to enhance visibility.
- Proactive threat hunting and attack surface reduction mandate threat intelligence feeds integration with SIEM/EDR and require periodic threat briefings.
- Compliance with internal security policies and industry best practices.
- All tickets must be created and tracked through Etisalat’s official ticketing portal to ensure proper documentation and accountability.
- Training and development for Etisalat's internal security team should be considered an integral part of the SecOps service and must be provided by the vendor at no additional cost. For more details, please refer to Section 3.2 – training and development Table.
- Vendors must sign and adhere to a Non-Disclosure Agreement (NDA) to ensure confidentiality and prevent exposure of any sensitive or proprietary information.
- The vendor shall perform both internal and external penetration testing twice a year as part of the SecOps engagement or during the implementation of major project implement. This service must be included at no additional cost and will be considered a value-added component in the evaluation of the vendor’s proposal. Providing this service will be viewed as a competitive advantage for a contract award.

Etisalat has various security solutions for monitoring in place as follows:

1) Vulnerability Scanners
2) Next Gen Firewalls
3) Web Application Firewalls (WAF)
4) Endpoint Detection & Response (EDR)
5) Network Detection & Response (NDR)
6) Privilage Access Managment (PAM)
7) Identity and Access Management (IAM)
8) Network Access Control (NAC)
9) Multi-Factor Authentication (MFA)
10) Zero Trust Network Access (ZTNA)
11) Firewall Analyzer
12) SIEM & SOAR
13) AD security tools

14) Threat intelligence

Note: Vendors are welcome to request additional information about the above tools by emailing the procurement team, who will coordinate with the relevant experts accordingly.

3.0 Scope of Work:

3.1. Security Monitoring & Threat Detection

- Continuous **24/7 monitoring** security logs, alerts, and telemetry from all tools like SIEM, SOAR, EDR, NDR andFirewall analyzer.
- Perform alert triage and correlation using Etisalat Afghanistan's centralized SIEM, EDR or a security analytics platform. **Vendors may also propose their own officially licensed tools for this purpose.**
- Proactive **threat hunting** to identify and mitigate advanced persistent threats (APTs).
- **Anomaly detection** through behavioral analysis and machine learning insights.
- Management and tuning of **use cases, correlation rules, and SIEM dashboards**.

3.2 Service requirements:

Bidders shall use the following options to indicate the "DEGREE OF SUPPORTOF COMPLIANCE" their service solution provides for each of requirements given in table below:

a. **FS - (Fully Supported)** The SecOps fully supports the requirement without any modifications.
b. **PS - (Partially Supported)** The SecOps supports the requirement with use of a system or workflow workaround.
c. **NS - (Not Supported)** The SecOps team is not capable of supporting the requirement and cannot be modified to accommodate the requirement.

Table 1: Service requirements for security operations and incident response

#	Category	Requirements	Response Time (SLA)	FS	PS	NS	Comments
1	Monitoring/Alert	Vendor should monitor security events to detect attacks and predict potential threats and raise alerts for any suspicious events that may lead to security	Immediate (Real-time Alerting)				

		breach in Etisalat environment. Monitor should be done on 24/7 basis with any or combination to the following operating modes remote/onside/office site/hybrid personnel					
2	Monitoring/Alert	Vendors must leverage the capability to detect and warn of incidents before they happen or at least at their early stages.	Immediate (Real-time Alerting)				
3	Monitoring/Alert	Vendor should alert Etisalat on any global security outbreaks that may threaten EA within 6 hours from it begin publicly known.	Immediate (Real-time Alerting)				
4	Monitoring/Alert	Must provide an acceptable false positive rate of detection not exceeding 5% total alerts raised	Immediate (Real-time Alerting)				
5	Monitoring/Alert	The vendor must be delivering the log analytic service to a large base of customers allowing to build knowledge based of know traits and common attack pattern	Immediate (Real-time Alerting)				

6	Alerts	Vendor security operations team should send alerts with details to designate personnel and systems upon detection of anomalies Alert types at least should be, emails, phone calls, Open a ticket. Describe your capabilities and strategy for reporting and alert	Immediate (Real-time Alerting)					
7	Log Analysis & Correlation	Vendor should analyze logs from multiple security devices (EDR, NDR, firewalls, SIEM, endpoints, etc.) to detect anomalies and threats.	Within 15 minutes of detection					
8	Incident Detection & Response	Vendor shall have an **Incident Response Framework** ensuring **containment, eradication, and recovery** of threats.	**Critical: < 12-24 hours** **High: < 24-48 hours** **Medium: < 48-120 hours** **Low: < 120-288 hours**					
9	Incident Response	Vendor must have clear classification of events, event types, severity, and impact to assess the severity once communicated to Etisalat Security team						
10	Incident Response	Describe your						

		incident response processes including the roles and responsibilities and scope of action					
11	Incident Response	Describe how you comply with international standards for incident responses. ISO/IEC 27035-1 Security incident management. NIST.SP.800-61 Computer security Incident Handling Guide. CSIRT, Computer Security Incident Response Team					
12	Incident Response	Vendor Should do root cause analysis for security incidents and recommend implementation of controls to prevent reoccurrence					
13	Incident Response	Vendor must share lesson learned from incidents affecting other customers (respecting privacy) and suggest fixes to our environment to avoid similar occurrences.					
14	Incident & investigation support	Vendor must provide on demand timely support to EA by performing					

		investigation and forensic analysis on the logs by doing the necessary analysis and log review and providing required data on a timely fashion					
15	Incident Management & Escalation	Vendor shall have a **structured escalation matrix** for critical incidents, ensuring immediate engagement with Etisalat's security team.	**Critical: < 30 minutes** **High: < 1 hour** **Others: < 2 hours**				
16	Forensic Analysis & Investigation	Vendor should provide **digital forensic capabilities** for in-depth analysis of security incidents.	**Preliminary Report: 24-48 hours** **Full Investigation: 5-7 days**				
17	Vulnerability Management	Vendor shall proactively **identify, assess, and report** vulnerabilities and provide actionable remediation.	**Critical: < 24 hours** **High: < 3 days** **Medium: < 7 days**				
18	Regulatory & Compliance Support	Vendor shall support compliance with **ISO 27001, NIST, GDPR**, and provide audit assistance.	**Audit Support within 5 business days**				
19	SOC Maturity & Continual Improvement	Vendor shall improve **SOC operations**, including automation of **threat detection,**	**Quarterly SOC Maturity Review**				

		incident response, and reporting.						
20	Third-Party & Supply Chain Risk Monitoring	Include supply chain threat monitoring (e.g., monitoring vendor access, shared log analysis).						
21	Cloud Security Monitoring	Vendor shall continues monitor the cloud services for identification and detection of relevant threats						
22	Reporting	**The vendor must provide security reports on a regular basis (or on-demand), tailored to technical, managerial, and executive audiences.** Reports should at least cover:<ul><li>SANS Top 6 log coverage (Authentication & Authorization, System/Data Changes, Network Activity, Resource Access, Malware Activity, Failure/Critical Errors)</li><li>**Compliance Reports** (ISO, PCI DSS, SOX, HIPAA, etc.)</li><li>**Network Situational Awareness Reports**	**Daily/Weekly /Monthly, On-Demand**					

		(top files, source/destination IPs, traffic anomalies, etc.)</li></ul>Please describe the distribution frequency (e.g., daily, weekly, monthly) and the content of each report					
23	Training & Development	The selected vendor shall provide continuous training and development support to enhance the capabilities of Etisalat Afghanistan's internal security team. The scope includes but is not limited to: • Conduct regular knowledge transfer sessions aligned with the services delivered (e.g., incident response, threat hunting, SIEM tuning, use case development). • Deliver hands-on workshops and scenario-based tabletop exercises to improve real-world incident handling capabilities.					

		Assist in skill development for use of any vendor-provided tools or platforms. • Recommend relevant cybersecurity certifications and career path guidance for SOC analysts and security engineers. • Enable shadowing opportunities where Etisalat team members can learn by observing or collaborating directly with the vendor’s expert teams during live incidents or threat investigations.					

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		

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

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

No.	Description	Compliance (YES/NO/NA)	Comments
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		
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	10. CONSTRUCTION OF CONTRACT:		
6	11. TERMINATION OF THE CONTRACT BY THE PURCHASER		
7	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 ================