EA Cybersecurity Requirements for the New Projects

Overview

This document defines the minimum Cybersecurity requirements that must be considered and incorporated in the RFx documents for new projects and systems. The Cybersecurity requirements are created in adherence to Etisalat Afghanistan Cybersecurity Policies.

The cybersecurity requirements outlined in our RFPs and contracts serve as the foundation of our commitment to safeguarding sensitive data and ensuring the integrity of our operations. Compliance with these measures is not just a formality but an essential component in mitigating risks, maintaining legal compliance, and protecting the trust of our stakeholders. By adhering to our cybersecurity protocols, vendors play a key role in strengthening our digital infrastructure against evolving threats, thereby contributing to a secure and resilient business ecosystem. We urge vendors to recognize the significance of these requirements and partner with us in upholding the highest standards of cybersecurity excellence.

Important Note

Bidders, vendors, project managers, 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 Afghanistan Cybersecurity Department.

For any compliant items, further supporting documents must be submitted to the Cybersecurity Department for analysis and validation.

No.	Description	Compliance (YES/NO/NA)	Comments
1	**Security Requirements**		
1.1	The Contractor/Supplier/vendor to sign Non-Disclosure Agreement (NDA) with Etisalat Afghanistan 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 Afghanistan's Cybersecurity Audit (Vulnerability Assessment/Penetration Testing/Security Audit) before go-live/service acceptance by Etisalat Afghanistan. Contractor/Supplier/vendor shall provide SLA for fixing Security gaps based on severity.		
1.4	Contractor/Supplier/vendor shall fix all security issues/vulnerabilities identified and reported by ETISALAT and/or Third Party Contracted to do the testing, with no additional cost even after going live.		
1.5	Contractor/Supplier/vendor confirms that its products/solution are tested for weaknesses via methods such as Vulnerability Assessment, penetration testing, Static/Dynamic Code Analysis, 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 Afghanistan.		

No.	Description	Compliance (YES/NO/NA)	Comments
1.6	The Contractor/Supplier/vendor shall provide evidence/report of the security assessment/audit of the proposed solution to Cybersecurity Department of Etisalat Afghanistan.		
1.7	Proposed system must not have dependency on end of life/end of support software or any such requirements.		
1.8	The proposed system (OS & Database) must be hardened with CIS control as per EA Secure Configuration Policy.		
1.9	Vendor must report any security incident or suspicious activity to Etisalat SOC team at soc@etisalat.af address.		
1.10	Vendor must ensure their operating systems/hardware are up to date and is not End of Life/End of support in next 3 years.		
1.11	EA has the right to request for vulnerabilities or penetration testing reports of web applications if vendor is supposed to deploy any in EA.		
1.12	The proposed system must not have any dependency on end of life/end of support software or any such requirements.		
1.13	Vendors must align all their services and configurations in accordance to EA Information Security policies and standards.		
1.14	Vendors must use and install only licensed applications.		
1.15	The installation and Integration of servers must be aligned with IT and Cybersecurity requirements.		
1.16	Vendor must access the servers only through Etisalat PAM solution.		
1.17	In the event of a security concern or suspicious activity arising from the vendor's end, Etisalat reserves the right to suspend or revoke access during investigation from Etisalat's side.		
1.18	Vendor must align their changes according to EA Change Management Policy.		
1.19	Vendor must ensure all their operating systems are fully patched with the latest OS/Software updates.		
1.20	The database must encrypt admin user's information with algorithms such as PBKDF2 and SHA256/384/512 bits.		
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 UAE NESA (SIA) IA V2, UAE DESC (ISR), UAE 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 that is not End of Life or End of Support.		

No.	Description	Compliance (YES/NO/NA)	Comments
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 and/or a standard Firewall Technology.		
2.4	The proposed solution shall not impact the existing Etisalat Afghanistan security controls or posture in any way.		
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 are strictly prohibited.		
3	**Password Security**		
3.1	All Operating Systems (e.g. Linux and Windows) must be hardened according to the official secure configuration baseline of Etisalat Afghanistan and to fully comply with Etisalat Afghanistan Security Policies.		
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/Threshold		
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	The hashing/encryption algorithm of the proposed solution must be in compliant with Etisalat Afghanistan cryptographic requirements.		
3.11	Forgetting or resetting password function must support MFA mechanism 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 integration with industry Privilege account Management (PAM) solutions.		
4.3	For public web applications, the proposed system supports and uses CAPTCHA or OTP to prevent against password attacks including but not limited to Dictionary Attack, Brute Force and Password Spraying mechanism.		

No.	Description	Compliance (YES/NO/NA)	Comments
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 including but not limited to FTP, Telnet, NTLM v1, and 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 were deemed necessary.		
4.9	The proposed solution shall support integration with Identity and Access Management solution (IAM) for user lifecycle management via standard APIs.		
4.10	The proposed solution must support LDAP and RADIUS authentication.		
5	**Authorization**		
5.1	The proposed solution shall support role-based and Rule 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 / rule-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 per Etisalat Afghanistan's Cybersecurity Policies		
6.5	The proposed system enforces input and output validation to prevent Cyber-attacks including but not limited to SQL Injection, Buffer Overflow, XSS and SSRF…etc.		
6.6	For web portals, the proposed solution shall include all the security controls to prevent / protect the application against 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) Source and Destination IPs d) Transaction ID & session information e) Failed/Successful Logins f) Modification of Security Settings g) Privilege Escalation h) User Account Modification		
7.3	The proposed solution shall support the integration with Etisalat Afghanistan NTP server for time synchronization and accurate logging.		
7.4	The proposed solution shall support integration with IBM QRadar for Log Aggregation and Correlation.		
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 in full compliance with Etisalat Afghanistan's Cryptographic requirements.		
8.2	The Public Cloud setup that stores PII information shall be hosted in the UAE		
8.3	The Public Cloud setup is hosted in a dedicated tenant for Etisalat Afghanistan (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 Afghanistan Cybersecurity Department		
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 Afghanistan's 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.		
10	**Artificial Intelligence and Machine Learning Security**		
10.1	If the proposed solution uses AI/ML, it must ensure model integrity, prevent model poisoning, and protect training data from leakage.		
10.2	Any AI model must be explainable and auditable, especially for systems impacting customer services or security decisions		
10.3	AI/ML-based systems must include monitoring to detect adversarial inputs or behavioral drift.		
10.4	Access to AI training datasets must be role-based and logged.		
11	**Encryption and Key Management**		
11.1	All sensitive data at rest and in transit must be encrypted using strong encryption standards (AES-256, TLS 1.3, etc.).		
11.2	Key management must be handled via secure KMS (Key Management Systems) in compliance with Etisalat Afghanistan's Cryptographic Policy.		
11.3	Private keys and credentials must not be hardcoded into applications or scripts.		
12	**Database Security**		
12.1	The database must enforce the least privilege of access and role separation.		
12.2	Database activity monitoring (DAM) should be enabled and integrated with the SIEM.		
12.3	Sensitive fields (e.g., PII, financials) must be encrypted and masking enabled for non-privileged users.		
12.4	Default accounts and unused stored procedures must be disabled or removed.		
13	**Network Security**		
13.1	The solution must comply with Etisalat Afghanistan's network segmentation and zero trust architecture.		
13.2	2 All network connections must be protected using firewalls, IDS/IPS, and NDR (Network Detection and Response).		
13.3	Insecure protocols (e.g., Telnet, SMBv1) must be disabled.		
13.4	Remote access must be restricted and controlled through VPN, MFA, and PAM.		
14	**API Security**		
14.1	APIs must enforce authentication and authorization using OAuth2.0 or JWT standards.		
14.2	APIs must be protected against OWASP API Top 10 vulnerabilities.		
14.3	API traffic must be logged and monitored with anomaly detection.		
14.4	Rate limiting and throttling mechanisms must be in place to prevent abuse.		

No.	Description	Compliance (YES/NO/NA)	Comments
15	**Physical and Environmental Security**		
15.1	Equipment housing critical data must reside in secure, access-controlled environments.		
15.2	Physical access to sensitive areas must be logged and monitored.		
15.3	Proper labeling, secure disposal, and asset lifecycle tracking must be implemented for all hardware.		
15.4	Surveillance and intrusion detection must be in place for all datacenter or server rooms used in the project.		
16	**Infrastructure and Visibility**		
16.1	All components of the infrastructure must support centralized logging and monitoring.		
16.2	The system must support integration with vulnerability scanners and patch management tools.		
16.3	Network and application topology must be documented and shared with EA Cybersecurity.		
16.4	Shadow IT and undocumented components must be reported and approved before deployment.		