TENDER NOTICE

No. EA/02-11-2026

For Cloud Backup Storage Capacity Expansion.

1. Bids are invited from Authorized Companies/Partners for Cloud Backup Storage Capacity Expansion. The Hard Bid Documents are also available in Etisalat head office and can be obtained from procurement department as well can download it from Etisalat Afghanistan website (www.etisalat.af, Tenders).

2. Bids shall be sent via email to snabizada@etisalat.af **Deadline: 16-February-2026**

Note: If you submit your commercial part of proposal by email, please provide it in **password protected document/format**. We will request the password once here the concerned committee started the bid's commercial evaluation.

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

4. Bidders should be registered with Etisalat Afghanistan in Vendor Registration List. If any interested bidder is not registered, first they should register their company before tender deadline and submission of bid.

5. Etisalat Afghanistan reserves the rights 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.

6. All correspondence on the subject may address to Shoaib Nabizada, Sr. Analyst Procurement & Contracts, Etisalat Afghanistan. Email snabizada@etisalat.af and Phone No.+93781 204113.

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

Request for Proposal (RFP)

For

Cloud Backup Storage Capacity Expansion

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 enumerated therein, such as the Conditions of Contract, the Deliverables, the Specifications and the Contractor's offer and correspondence relating thereto, the Bill of Quantities with unit prices to be provided by the Contractor after completion of the detailed design work, (where applicable) or as approved by EA based on the accepted bid with agreed to adjustments Appendices and Addenda as well as any amendments made to any such documents in accordance with the Contract.

"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.

For the purpose of clarification, D.D.P Price here means that all costs, expenses, duties and taxes, incurred or payable on Goods by the contractor up to the point the Goods are handed over to consignee/ultimate consignee, are included in the price of the Goods.

"Documentation" means documentation specified in the relevant Article(s).

"Drawings" means the drawings referred to in the Contract documents and any modification of such drawings approved in writing by EA and such other drawings as may from time to time be furnished or approved in writing by EA.

"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 republic 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" means raw materials, products, equipment, systems, spares, and commodities in solid, liquid or gaseous form, and electricity, incidental services, transport, maintenance and similar obligations related to the supply of Goods if the value of those services does not exceed the value of the Goods themselves. The Goods include all of the equipment, machinery, and/or other materials which the Contractor is required to supply to EA under the Contract as per EA Technical Specifications.

"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.

"Pre-Shipment Inspection" means inspection and testing of Goods at manufacturer's premises in accordance with the provisions of the specifications and the clause(s) of the contract pertaining to Pre-shipment Inspection.

"Prime Contractor" means the individual or firm ultimately responsible for supplying all the Goods on time and to cost under this Contract to EA.

"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.

"Shipping Documents" means Contractor's Valued Invoice, Packing List, Freight Memo (if any), Weight and Measurement Certificate, Original Bill of Lading or Airway Bill (as the case may be), Certificate of Origin, Warranty Certificate, Insurance Declaration and Inspection Certificate and/or Contractor's Factory Test Certificate, as required by the 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.

"Site" means the land or locations, buildings and other places including containers shells wherein and upon which the Goods are to be supplied/delivered, and such other land or places as may be specified in the Contract as forming part of the site.

"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.

"Subcontractor including Vendors" means any person to whom execution of any part of the facilities and/or services including preparation of any design or supply of any plant and equipment, is sub-contracted directly or indirectly by the Contractor, and includes its legal successors or permitted assigns.

"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 warehouse or site certified by EA authorized representative (s).

2. INTRODUCTION TO WORK.

2.1 Offer invited for Cloud Backup Storage Capacity Expansion. in accordance with Etisalat specifications as per **Annexure A.**

2.2 Cybersecurity clauses as per **Annexure B.**

3. Scope of Work

As per Annexure –A

4. Validity of Offers

The offer 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. Registration/Legal documents of the Bidder:

The Bidder shall include in his proposal, copies of registration documents such as the Certificate of Registration, Trade License, Chamber of Commerce Certificates, and Memorandum of Association (for Limited Liability Company) which shall be legalized as follows:

6. Progress of Work:

6.1 The Contractor shall commence the execution of the Contract and shall proceed in an orderly and proper manner with due expedition and without delay in order to ensure that the services/activities/jobs as stipulated in the contract are completed by the specified Completion Date.

6.2 A Progress Report shall be submitted by the Contractor showing the progress, any anticipated delays and any other relevant information. Each Progress Report shall include a statement confirming that the services/activities/jobs or part thereof shall be completed by the specified date or a detailed explanation, should delay be anticipated.

6.3 The Contractor shall be responsible for the quality of work and the execution of the Project and provision of services as per annexure-A. The Purchaser reserves the right to ensure such control and supervision as is deemed necessary.

7. Price

7.1 Price shall be quoted on in Afghani Currency or USD.

7.2 The price shall be inclusive of all taxes applicable as per Afghanistan Government Tax Laws on Services including Withholding Tax.

8. Payment Terms.

8.1 EA will make 100% payment after delivery of hardware and software/license.

8.2 Advance payment will be not made to contractor.

8.3 Payment will be made through Bank Transfer.

8.4 EA shall make prompt payment, within thirty (30) days of submission of an invoice/claim by the contractor subject to availability of pre requisite documents specified under the contract and adjustment of penalty (if any) on account of late delivery and/or defective Goods replacement after confirmation from Project Director.

8.5 Payments are subject to deduction of income tax at 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 certificate of deductions to the contractor to enable him to settle tax returns with the concerned authorities.

9. Construction of Contract:

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

10. Termination of the Contract by the Purchaser:

10.1 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.

10.2 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.

11. Termination of the Contract by the Contractor:

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

11.2 In the event of the Contract being terminated by the Contractor as indicated, the Contract Price payable by the Purchaser to the Contractor (after taking into account amounts previously paid under the Contract) shall be the Price, as specified in the Contract, of the services received and accepted at the date of termination.

12. Local Taxes, Dues and Levies:

12.1 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.

12.2 Withholding tax (if applicable) shall be deducted on local portion only as per prevailing rates as notified Islamic republic 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.

13. Settlement of disputes:

13.1 All disputes arising out of or in connection with this Contract shall be finally decided by the Courts of Islamic Republic of Afghanistan. Such decision shall be binding to parties. For this purpose the parties shall be deemed to have agreed to submit to the jurisdiction of the Courts of Islamic Republic of Afghanistan and to have waived any immunity that may be claimed in this respect.

13.2 Notwithstanding that a dispute may have been referred to the Court both parties shall, if required by the Purchaser, proceed with their contractual obligations.

14. Corrupt Practices:

14.1 The Contractor shall not offer or give or agree to give to any person any gift or consideration of any kind as an inducement or reward for doing of fore-bearing to do or for having done or forborne to do any act in relation to the obtaining or execution of this or any other Contract with the Purchaser or for showing or forbearing to show favor or disfavor to any person in relation to this or any other Contract with the Purchaser.

14.2 The Contractor shall not enter into this or any other Contract with the Purchaser in the event that any such commission has been paid or agreed to be paid by him or on his behalf or to his knowledge, unless before the Contract is made, particulars of any such commission and of terms and conditions of any agreement for the payment thereof have been disclosed in writing to the Purchaser.

14.3 Any breach of this condition by the Contractor or by anyone employed by him or acting on his behalf (whether with or without the knowledge of the Contractor) shall entitle the Purchaser to terminate the Contract.

15. Publicity and confidentiality

15.1 The Contractor shall not, and shall ensure that none of his sub-contractors will, advertise or otherwise disclose the appointment of the Contractor or his sub-contractors or the terms of the Contract (save insofar as may be required by law or may be necessary for the due performance of the Contract) without the prior approval in writing of the Purchaser. All copy of material relating to this Contract which is intended for publication in any form by the Contractor or any sub-contractor must first be submitted in draft form to the Purchaser for approval indicating the countries in which it will appear.

15.2 The Contractor shall ensure that he and / or his sub-contractors (including their personnel) shall not disclose the location, nature, purpose, details of equipment; technical specifications, customized /tailored designs etc. or other confidential / site specific information given to him as a result of awarding the Contract or gained by him from his association with other Contractors of the Purchaser in the same site, area or field to a third party, without obtaining prior approval in writing from the Purchaser.

Annexure – A

Organization Background – Etisalat Afghanistan

Etisalat Afghanistan operates a large-scale, mission-critical telecommunications environment supporting enterprise, consumer, and regulatory workloads. The organization relies heavily on **Microsoft 365 and SaaS platforms** for daily operations, collaboration, customer support, and compliance-driven communications.

To ensure **business continuity, regulatory compliance, ransomware resilience, and long-term data governance**, Etisalat Afghanistan has deployed **Dell EMC / Druva SaaS Backup Services** under an **Enterprise Agreement (EA)**. This service currently protects Microsoft 365 workloads and is fully operational in production.

Etisalat Afghanistan is issuing this RFP to **enhance and extend existing data protection capabilities** or **introduce an on-premises backup model using existing Data Domain infrastructure**, without disrupting ongoing operations.

RFP Objective

The primary objective of this RFP is to:

- Enhance Microsoft 365 and SaaS data protection capacity and capabilities
- Support future data growth while maintaining operational stability
- Strengthen ransomware protection, immutability, and long-term retention
- Ensure compliance with Etisalat Group security, governance, and audit requirements
- Optimize licensing, cost transparency, and scalability over a **4-year planning horizon**

Vendors are invited to propose solutions under **one or both options**, clearly identifying the proposed approach, assumptions, and commercial models.

Option 1 – SaaS Backup Capacity Expansion (Existing Service Enhancement)

Objective

Increase backup storage capacity for existing licensed users **without changing the current Dell EMC / Druva backup service architecture, platform, or operational model**.

Key Clarifications

- **Dell EMC / Druva Backup Services are currently running in production**

- **No platform replacement, migration, or architectural change is allowed**
- The scope is strictly limited to **capacity enhancement or capacity-consumption model optimization**
- Existing policies, integrations, and backup configurations must remain intact

Capacity Enhancement Models (Vendor May Propose One or More)

Vendors may propose **alternative capacity models**, including but not limited to:

- High-capacity tier upgrade
- Additional fixed storage capacity (e.g., +50 TB)
- Storage consumption-based model
- Druva credit-based or usage-based consumption model
- Hybrid capacity + consumption model

The proposed model must:

- Support **754 existing licensed users**
- Provide **up to 50 TB additional effective capacity**
- Be valid for **4 years**
- Be priced on a **yearly basis**
- Align with the existing **EA expiring on 01 February 2029**
- Clearly explain how capacity is calculated, consumed, and monitored

Commercial Expectations

- Year-by-year pricing for the full 4-year term
- Clear explanation of capacity calculation methodology
- Confirmation that no additional user licenses are required
- Explicit confirmation that the existing Dell EMC / Druva service remains unchanged

Option 2 – On-Premises Data Domain–Based Backup Solution

Objective

Provide a **complete end-to-end cloud data protection solution** using the organization's **existing on-premises Dell EMC Data Domain systems** as the primary backup repository.

Current Environment

- Cloud data size: **40 TB**
- Estimated annual data growth: **15–20%**
- Total users: **881**
- Existing Data Domain systems:
  - **DD6900 – 250 TB**
  - **DD6900 – 170 TB**
  - **DD6400 – 81 TB**

Key Requirements

- Backup Microsoft 365 data directly to on-premises Data Domain
- End-to-end coverage including ingestion, retention, recovery, immutability, and ransomware protection
- Licensing model must be **clearly defined**
- Separate pricing for:
  - Licenses
  - Support & maintenance
- Pricing must be **yearly base** for **4 years**
- Support existing Data Domain deduplication, compression, and immutability features

---

Consolidated Statement of Work (SOW)

Requirement Description	Comply	Not Comply
Backup of active and archived mailboxes, including all message content and metadata	☐	☐
Backup of public folder mailboxes	☐	☐
Backup of shared mailboxes without requiring active user licenses	☐	☐
The solution should provide granular (single object) backup and restore capabilities.	☐	☐
Backup of all mailbox attachments regardless of size or type	☐	☐
Backup of SharePoint Online site collections including all content types	☐	☐
Preservation of SharePoint site hierarchies and structures	☐	☐
Backup and recovery of SharePoint permissions and access controls	☐	☐
Backup of OneDrive for Business site collections	☐	☐
Backup of Microsoft Teams and M365 Groups document libraries	☐	☐
Backup of Teams conversations and chat history	☐	☐
Backup of all files shared through Teams conversations	☐	☐
Backup of Teams wikis and related collaboration data	☐	☐
Item-level, folder-level, mailbox-level, and site-level recovery	☐	☐
Ability to restore multiple mailboxes in a single operation	☐	☐
Recovery to alternate locations, including cross-tenant and on-premises Exchange or SharePoint	☐	☐
Advanced recovery filtering (date, user, object type, keyword, etc.)	☐	☐
Access to former employees’ data without maintaining active licenses	☐	☐

==

Requirement Description	Comply	Not Comply
Continuous or near-continuous data protection with automated backups	□	□
Archive storage support for former employees' data	□	□
Ransomware recovery capabilities including point-in-time restores	□	□
Long-term retention policies configurable per workload	□	□
Immutable backup storage support	□	□
The solution should consider the standard security framework for backup /recovery	□	□
Support for Exchange Online, SharePoint Online, OneDrive, and Microsoft Teams including metadata and security attributes	□	□
Clear breakdown of all licensing costs, recurring fees, and support charges	□	□
Explicit description of licensing model (per user, per TB, per object, or hybrid)	□	□
Post-implementation support coverage and SLAs	□	□
Administrator training should be included as a FOC	□	□
Integration with existing on-premises Dell EMC Data Domain systems (DD6900, DD6400)	□	□
Use of Data Domain as the primary backup repository	□	□
Enablement of Data Domain deduplication and compression	□	□
Encryption of data in transit and at rest	□	□
Alignment with Microsoft 365 Shared Responsibility Model and data governance requirements	□	□
Detailed solution architecture diagram and technical explanation	□	□
Implementation plan including timeline, sizing assumptions, and capacity calculations	□	□
Yearly pricing breakdown for a 4-year term for License and Support.	□	□

Annexure-B

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.

S.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.		
1.6	The Contractor/Supplier/vendor shall provide evidence/report of the security assessment/audit of the		

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

S.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.		

S.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…		

S.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.		

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

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

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 Doc*************************************