TENDER NOTICE

No: EA/02-07-2024

For Developing an Enterprise App

1. Bids are invited from well-reputed companies for developing an enterprise app for Etisalat Afghanistan. The hard bid Documents are also available at Etisalat head office and can be obtained from the procurement department or downloaded from the Etisalat Afghanistan website (www.etisalat.af, Tenders).

2. Bidders are requested to send the proposals/offers via email to ghurzang@etisalat.af by **29 February 2024**.

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

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

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

5. 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.

6. All correspondence on the subject may address to Ghurzang Waziri, Sr. Specialist Procurement & Contracts, and Etisalat Afghanistan. Email ghurzang@etisalat.af and Phone No. +93781 204068.

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

==========

Request for Proposal

(RFP)

For

Developing an Enterprise App

1. DEFINITIONS

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

1.1 Terms.

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

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

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

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

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

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

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

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

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

"Contract" means the Contract between Etisalat Afghanistan (EA) and the Contractor and comprising documents 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 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 the 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 the Islamic Republic of Afghanistan and has an office at Ihsan Plaza Charahi Shaheed Kabul in person or any person duly authorized by it for the specific purpose for the specific task within the Contract and notified to a 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 the 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 a 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 the successful bidder with regard to the award of the 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 to 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 are substantially different in basic characteristics or in purpose or utility from its components.

"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.

"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.

"Warranty Period" shall mean the period of 3 months or any extended period starting from the acceptance of the delivered goods in good order and conditions at the consignee's warehouse or site certified by EA authorized representative (s).

2. Scope of Work

The scope of work is as per Annexure A.

3. Validity of Offers

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

4. Price

4.1 Price shall be quoted on a Unit Rate basis in Afghanis OR USD. Prices quoted in other currencies will cause rejection of your bid.

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

5. Payment Terms.

5.1 Payment shall be made to Contractor on a monthly basis as per contracted price at the end of the calendar month for which items are provided and verified by an authorized EA representative.

5.2 Payment shall be made against invoice to be submitted by Contractor within thirty (30) days of submission of invoice.

5.3 No advance payment will be made to the contractor.

6. Penalty:

6.1 If the contractor fails to supply the said items 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 the Total PO price of the delayed PO for each week and pro-rata for parts of the week, for delay beyond the specified date, subject to a maximum of ten percent (10%) of the Total PO Price. If the delay is only in respect of small items that do not affect the effective utilization of the system, the penalty shall be chargeable only on the value of such delayed items.

6.2 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

7. Construction of Contract:

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

8. Termination of the Contract:

8.1 Etisalat has the right in the event of earlier termination of the contract. Etisalat may serve thirty (30) days prior notice in writing to the Contractor.

8.2 Also if the Contractor fails to deliver any or all of the deliverables within the time period specified in the contract or any extension thereof granted by ETISALAT.

9. Local Taxes, Dues, and Levies:

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

9.2 The amount of withholding Tax(s) is 2% of all project costs for local/registered companies who have Afghanistan Government Official Work License and 7% for International/ non-registered companies.

Annexure –A

Scope of Work for Developing an Enterprise App

To develop an exclusive app for enterprise with key features against

Super Admin- Super admin will have the master rights

Admin- Admin will have functional rights

Reset Options- All reset trials will reach Super Admin's email for approval

REQUIREMENTS AND SCOPE OF WORK:

- Options to view the summary of total connections/Active Count/ Billing
- Graphical representation of the organization & status of MSISDNs
- Summary of total billing/ Last paid amount
- Options to view the count of MSISDNs having CUG/International roaming
- Options to click on the tab and view further details
- Options to restrict view for Admin & Super Admin
- Employee to view the summary of his MSISDN
- Admin to view the summary of his function
- Super Admin to have the master view
- MSISDN-wise, view of employees/ Service opted/CUG/ IR/ Package name/Payment status, etc…
- DIY(Do It Yourself) options to configure the services MSISDN-wise

i. Introduction:

In today's dynamic business landscape, staying ahead requires innovation and adaptability. At Etisalat Afghanistan, we understand the pivotal role technology plays in driving success and fostering growth.

We are seeking proposals from experienced and innovative vendors who can collaborate with us to bring this vision to life. This mobile app aims to revolutionize how businesses interact with their customers and streamline internal operations, ultimately driving growth and success:

==========

- **Opportunity for Collaboration**:

  This RFP presents an exciting opportunity for vendors to partner with us on a transformative project that promises to redefine industry standards and unlock new opportunities. We are committed to fostering collaborative relationships built on trust, expertise, and shared objectives.

- **Vision for the Mobile App:**

  Our vision for this mobile app is rooted in enhancing customer experiences, providing self-service functionalities, and optimizing operational efficiency. We believe that through strategic collaboration with the right vendor, we can turn this vision into reality and deliver a solution that exceeds expectations.

- **Scope of Work:**

  Vendors are invited to submit proposals outlining their approach to developing the mobile app, including technical expertise, project management capabilities, and proposed timelines. We are particularly interested in innovative solutions that demonstrate a deep understanding of our business goals and customer needs.

- **Target Platforms and Compatibility:**

  The mobile app should be compatible with both iOS and Android platforms, ensuring seamless performance across various devices. Vendors are encouraged to propose solutions that maximize accessibility and usability, catering to a diverse user base.

List of Key Features:

- **User Registration and Authentication**: Enable users to create accounts and securely log in using authentication mechanisms.
- **Support Multi-Factor Authentication (MFA):** Implement additional layers of security to verify user identities and protect against unauthorized access.
- **User Profiles and Settings:** Allow users to manage their profiles, preferences, and account settings.
- **Push Notifications:** Deliver real-time notifications to users, keeping them informed and engaged.

==========

- **Version Control:** Ensure seamless management of app versions to facilitate updates and enhancements.
- **Integration with Third-Party Services:** Integrate with external services and APIs to extend functionality and access additional features.
- **Data Synchronization:** Enable synchronization of data across devices and platforms to ensure consistency and continuity of user experience.
- **Offline Availability:** Provide offline access to essential features and content, allowing users to use the app even without an internet connection.
- **Location-Based Services:** Utilize location data to deliver personalized experiences, relevant content, and location-based functionalities.
- **Multimedia Support:** Support various multimedia formats, including audio, video, and images, to enrich user interactions and content consumption.
- **Search Functionality:** Implement robust search capabilities to help users find information, products, or services quickly and efficiently.
- **Analytics and Reporting:** Incorporate analytics tools to track user behavior, gather insights, and generate reports for data-driven decision-making.
- **Admin Panel or Content Management System (CMS):** Provide an intuitive interface for administrators to manage app content, users, and settings efficiently.

User Interface (UI) and User Experience (UX):

- **Branding and Theming:** Reflect the branding guidelines and color schemes of Etisalat Afghanistan to maintain consistency and reinforce brand identity.
- **Interactive Elements:** Implement intuitive and responsive design elements to enhance usability and engagement.
- **Animations and Transitions:** Utilize subtle animations and transitions to create a fluid and visually appealing user experience, improving navigation and feedback.

b. UI and UX Design Principles:

The UI and UX design should align with the specific themes, color schemes, and branding guidelines of Etisalat Afghanistan, reflecting a cohesive and visually appealing interface.

==========

c. Enhancing User Experience:

Incorporate animations, transitions, and interactive elements strategically to elevate the user experience, making interactions intuitive, engaging, and memorable.

This revised version provides a more detailed and structured overview of the features and functionality, as well as specific guidelines for UI/UX design principles to ensure alignment with Etisalat Afghanistan's branding and enhance user experience.

ii. **Technical Requirements:**

1. Required Technologies and Frameworks:

- **Programming Languages**: Utilize appropriate programming languages such as Swift for iOS, Kotlin for Android, Huawei or React Native for cross-platform development to ensure optimal performance and compatibility.
- **Development Tools**: Employ industry-standard development tools such as Xcode, Android Studio, and Visual Studio Code for efficient development, testing, and debugging across platforms.
- **Backend Technologies:** Implement robust backend technologies including RESTful APIs and server-side scripting languages like Node.js or Python to facilitate seamless communication between the mobile app and backend systems.
- **Database Management Systems**: Choose suitable database management systems like MySQL, Firebase, or MongoDB to efficiently store, retrieve, and manage app data while ensuring scalability and reliability.
- **Cloud Services:** Leverage cloud services such as AWS , Azur or Google Cloud Platform to host the backend infrastructure, ensuring scalability, security, and high availability.

b. Minimum Hardware and Software Specifications:

- **Device Compatibility:** Ensure the app functions optimally on target devices by defining minimum hardware specifications such as processor speed, RAM, and screen resolution to deliver a smooth and responsive user experience.
- **Operating System Compatibility:** Support the latest versions of iOS and Android platforms to maximize compatibility with a wide range of devices and ensure access to the latest features and security enhancements.

==========

2. Integration and Data Exchange:

- **Telecom Billing Systems Integration:** Integrate with telecom billing systems to provide timely billing information for services acquired, including international roaming numbers, CUG numbers, and total connections/Active Counts, ensuring accurate and transparent billing processes.
- **Customer Relationship Management (CRM) System Integration:** Seamlessly integrate with the Customer Relationship Management (CRM) system to centralize customer data, improve customer interactions, and enhance overall customer service and management processes.
- **Service Delivery Platform (SDP) Integration:** Integrate with Etisalat SDP platform to manage subscriptions and lifecycles management for different services through different channels.
- **CPaaS Voice & SMS APIs and Bulk SMS API Integration:** Integrate with Communication Platform as a Service (CPaaS) Voice & SMS APIs and Bulk SMS API to enable voice and text communication functionalities within the app, facilitating seamless communication with users.
- **Real-time Push Notifications Integration:** Integrate with relevant systems for sending transactional real-time push notifications, alerts, and targeted personalized notifications to app users, ensuring timely and engaging communication.
- **Third-Party APIs Integration:** Integrate with relevant APIs of third-party services and systems to exchange data securely and efficiently, detailing the protocols and data formats to be used to ensure seamless interoperability and data exchange.
- **Payment Service Providers Integration:** Integrate with MFS (Mobile financial System) and payment service providers to facilitate secure and seamless payment transactions within the app, ensuring a frictionless user experience and adherence to payment security standards.
- **Social Media Integration**: Integrate social media accounts to enable users to share app content on social platforms, extending the app's reach and enhancing user engagement through social sharing functionalities.

==========

- **Geo-location Integration:** Integrate with relevant systems in the EA Network to fetch geo-location for location-based services, enabling personalized and context-aware experiences based on user location.
- **Data Security and Encryption:** Ensure that data exchange between the mobile app and backend systems is encrypted to safeguard sensitive information and uphold data security standards, mitigating the risk of unauthorized access or data breaches.
- **Data Synchronization Mechanisms**: Implement mechanisms to synchronize data between the mobile app and integrated systems, ensuring consistency and real-time updates across all platforms, enhancing data accuracy and user experience.
- **Standard APIs Supportability**: Ensure support for standard APIs for third-party integrations, enabling seamless integration with external systems and services, facilitating scalability and interoperability.

3. Testing and Quality Assurance:

- **Comprehensive Integration Testing:** Conduct thorough testing to ensure smooth integration between the app and third party services. Verify data exchange, functionality, and compatibility to guarantee a seamless and error-free user experience.
- **Security Verification:** Verify the security of data exchanges and integrations through rigorous penetration testing, vulnerability assessments, and adherence to industry best practices. Ensure that the app maintains robust security protocols to safeguard user data.
- **Testing Approach:** Develop a comprehensive testing approach that includes:
  - ✓ Unit Testing: Verify the functionality of individual components to ensure they operate as intended.
  - ✓ Integration Testing: Validate the interactions and interoperability between different modules and systems.
- **User Acceptance Testing (UAT):** Engage end-users to evaluate the app's usability and ensure it meets their expectations and requirements.
- **Performance Testing:** Perform performance testing to assess how the app performs when interacting with integrated systems and third-party services under various loads

and scenarios. This includes evaluating response times, scalability, and resource utilization.

- **Quality Assurance Processes:** Implement robust quality assurance processes to ensure the app meets specified requirements and adheres to industry best practices. This includes:
- **Code Reviews:** Regularly review code to identify and rectify potential issues and ensure adherence to coding standards.
    - ✓ Test Automation: Implement automated testing to streamline the testing process, improve efficiency, and identify regressions.
    - ✓ Continuous Integration/Continuous Deployment (CI/CD): Establish CI/CD pipelines to automate testing and deployment processes, promoting continuous improvement and efficiency.

4. Deployment and Release:

a. Deployment Process: The deployment process for the app should adhere to the submission guidelines of app stores, including Apple App Store for iOS and Google Play Store for Android. This includes:

- ✓ Compliance with platform-specific requirements, such as app content guidelines, metadata requirements, and technical specifications.
- ✓ Preparation of necessary assets, including app icons, screenshots, descriptions, and promotional materials.
- ✓ Submission of the app for review and approval by the respective app store authorities.
- ✓ Define release milestones to track progress throughout the deployment process, including:
- ✓ Prototype Delivery: Submission of initial app versions for internal testing and feedback.
- ✓ Beta Testing: Distribution of pre-release versions to a select group of users for testing and validation.
- ✓ Final Release: Deployment of the app-to-app stores for public availability.

b. Post-Release Support:

The release should support post-release activities, including:

- ✓ Bug Fixes: Prompt identification and resolution of any issues or bugs discovered post-release, ensuring the app's stability and reliability.
- ✓ Updates: Regular updates to add new features, improve performance, address user feedback, and stay aligned with evolving platform requirements.
- ✓ Versioning: Implementation of versioning strategies to track app releases and maintain clarity regarding the app's current state and history.

5. Documentation and Training:

a. Documentation:

- **User Manuals:** Provide comprehensive user manuals that offer step-by-step instructions on using the app, including how to navigate its features, perform common tasks, and troubleshoot issues.
- **Technical Specifications:** Deliver detailed technical specifications documentation that outlines the architecture, components, and functionalities of the app, providing insights for developers and administrators.
- **API Documentation:** Include thorough documentation for APIs used within the app, detailing endpoints, request/response formats, authentication mechanisms, and usage guidelines to facilitate integration and development processes.

b. Training:

- **User Training:** Conduct training sessions for app users to familiarize them with its features, functionalities, and best practices for optimal usage. Offer interactive tutorials, walkthroughs, and Q&A sessions to ensure users feel confident and empowered in utilizing the app effectively.
- **Administrator Training:** Provide specialized training for administrators responsible for managing app settings, user accounts, content, and other administrative tasks. Cover topics such as backend management, analytics interpretation, and maintenance procedures to empower administrators with the necessary skills and knowledge.

- **Developer Training:** Offer training sessions for developers involved in app maintenance, customization, and future enhancements. Provide insights into the app's architecture, coding standards, version control practices, and debugging techniques to ensure developers are equipped to maintain and extend the app effectively.

6. Post implementation and Maintenance Support Services

Post-implementation and maintenance support services are crucial for ensuring the long-term success and sustainability of the mobile app:

- **Bug Fixes and Issue Resolution:** Provide timely bug fixes and issue resolution services to address any technical issues or performance concerns that arise after the app's deployment. This includes identifying, prioritizing, and resolving bugs reported by users or detected through monitoring tools.
- **Updates and Enhancements:** Offer regular updates and enhancements to the app to introduce new features, improve performance, address user feedback, and stay aligned with evolving platform requirements. This may involve version upgrades, feature enhancements, and optimizations based on user analytics and market trends.
- **Technical Support:** Provide ongoing technical support to assist users and administrators with troubleshooting, guidance, and assistance in using the app effectively. This includes offering responsive communication channels, such as helpdesk support, email support, or live chat, to address queries and concerns promptly.
- **Security Updates and Compliance:** Stay proactive in implementing security updates and patches to address emerging threats and vulnerabilities, ensuring the app remains secure and compliant with industry standards and regulations. This includes regular security audits, vulnerability assessments, and adherence to best practices in data security and privacy**.**
- **Performance Monitoring and Optimization:** Continuously monitor the app's performance metrics, including response times, server uptime, and user feedback, to identify areas for optimization and improvement. This may involve performance tuning, resource optimization, and scalability enhancements to maintain optimal app performance under varying loads and conditions.

==========

- **Backup and Disaster Recovery:** Implement robust backup and disaster recovery procedures to safeguard app data and ensure business continuity in the event of unforeseen incidents or disasters. This includes regular data backups, offsite storage, and recovery protocols to minimize downtime and data loss risks**.**

7. Service Level Agreements (SLAs) and Reporting:

Define clear service level agreements (SLAs) outlining the response times, resolution times, and support availability for different types of support requests. Regularly report on key performance indicators (KPIs), service metrics, and adherence to SLAs to ensure transparency and accountability in service delivery.

Cybersecurity Requirements for the New Projects / Systems

Overview

This document is defining 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.

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 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.		

==========

No.	Description	Compliance (YES/NO/NA)	Comments
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		
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. The Contractor/Supplier/vendor shall provide evidence/report of the security assessment/audit of the proposed solution to Cybersecurity Department of Etisalat Afghanistan.		
2	**Security Architecture**		

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

No.	Description	Compliance (YES/NO/NA)	Comments
	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.		
3.10	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.		

==========

No.	Description	Compliance (YES/NO/NA)	Comments
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.		
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 where deemed necessary.		
4.9	The proposed solution shall support integration with Identity and Access Management solution (IAM) for user lifecycle management via standard APIs.		
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		

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

The following Information must be submitted with the offer:

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	
Company Financial Statement/bank statement for last two years	
Experience over the last two years	

==========