TENDER NOTICE

No. EA/02-10-2024

For Providing of ADMS (Automatic Device Management System)

1. Bids are invited from potential Companies for Providing ADMS (Automatic Device Management System) in Afghanistan as per RFP Annexure. This bid Document is also available on the Etisalat website (www.etisalat.af, Tenders).

2. RFP Deadline is 18 March 2024 Afghanistan time. The bids shall be submitted through email (ashalizi@etisalat.af) and marked clearly with the **RFP name, and number.**

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

4. Local and international firms can send their offer via email to ashalizi@etisalat.af and copy Ihsanullah@etisalat.af.

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. The bidder shall submit proposal with separate (Technical and Commercial) parts. The commercial part must be password protected document and we will request the password once here the concerned committee opened bids (start bid's Commercial evaluation). The bids shall be first evaluated technically. Technical evaluation will be based on the conformity to required technical specifications and compliance matrix specified in the Bidding Documents. Only technically compliant bids that meet all the mandatory service-effecting requirements will be evaluated commercially.

7. Bidder should be registered with Etisalat Afghanistan in Vendor Registration List. If any interested bidder **is not registered**, first they should fill the attached Vendor Registration Form and provide following documents before tender deadline and submission of bid. Bidder's offer will not be considered without the registration process**.**

1- Company Profile
2- Business License
3- President and Vice President ID Cards/Tazkira Copies
4- Article of Association (اساس نامه)
3. Past Performance:

Firm must describe past performance on similar public and or private agency contracts, including past performance on similar works for any other telecom company.

8. All correspondence on the subject may address to Ahmad Shikib Shalizi, Specialist Procurement, and Etisalat Afghanistan. Email ashalizi@etisalat.af and Phone No. +93781 204 040.

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

Providing ADMS Solution (Automatic Device Management System) for Etisalat Afghanistan

1. DEFINITIONS

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

1.1 Terms.

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

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

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

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

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

"Bid/Tender Document" means the Bid/Tender documents issued by EA for invitation of Bids/Offers along with subsequent amendments and clarifications.
"CIF" means "Cost Insurance Freight" as specified in INCOTERM 2010.

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

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

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

"Contract" means the Contract between Etisalat Afghanistan (EA) and the Contractor and comprising documents.

"Contractor" means the individual or firm(s) ultimately responsible for supplying all the Goods/Equipment/Systems/Material/Items on time and to cost under this contract to EA.

“Contractor’s Representative” means the person nominated by the contractor and named as such in the contract and approved by EA in the manner provided in the contract.

“Contract Documents” means the documents listed in Article (Contract Documents) of the Form of Contract (including any amendments thereto) or in any other article in this contract.

“**Contract Price”** means the price payable to the Contractor under the Contract for the full and proper performance of its contractual obligations.

“Day” means calendar day of the Gregorian calendar.

“Delivery charges” means local transportation, handling, insurance and other charges incidental to the delivery of Goods to their final destination.

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

“Effective Date” means the date the Contract shall take effect as mentioned in the Contract.

“Etisalat Afghanistan (EA)” means the company registered under the Laws of Islamic 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 Receipt Certificate” means certificate issued by the consignee certifying receipt of Goods in good order and condition.

“Liquidated Damages” mean the monetary damages imposed upon the contractor and the money payable to EA by the contractor on account of late delivery of the whole or part of the Goods.

“**L.o.A**” means Letter of Award issued by EA to successful bidder with regard to the award of tender.

“Month” means calendar month of the Gregorian calendar.

“Offer” means the quotation/bid and all subsequent clarifications submitted by the Bidder and accepted by EA in response to and in relation with the Bid Documents.

“Origin” means the place where the Goods are mined, grown or produced from which the ancillary services are supplied. Goods are produced when, through manufacturing, processing or substantial and major assembling of components, a commercially recognized product results that is substantially different in basic characteristics or in purpose or utility from its components.

“EA's Representative” shall mean the representative to be appointed by EA to act for and on behalf of EA with respect to this Contract.

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

“Supplier/Vendor” (used interchangeably) means the individual or firm ultimately responsible for supplying all the Goods on time and to cost under this Contract acting individually alone or as a “prime contractor” for a consortium.

“Supplier's Representative” means the person nominated by the Contractor and named as such in the Contract and approved by EA in the manner provided in the Contract.

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

2. INTRODUCTION TO WORK.

2.1 Bids are invited for Providing ADMS (Automatic Device Management System) in accordance with Etisalat specifications as per Annexure A and B.

3. Bill of Quantity (BoQ)

As per Annexure –A

4. Validity of Offers

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

5. Price and Payment Term

5.1 Payment shall be made by bank transfer after receipt of original Hardcopy of invoice.
5.2 Advance payment shall be not made to the contractor.
5.3 EA shall make prompt payment, within thirty days of submission of an invoice/claim by the contractor subject to availability of prerequisite documents specified under the contract and adjustment of penalty (if any) on account of late delivery and/or defective Goods replacement after confirmation from Project Director.

5.4 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.

5.5 Payments against the entire contract will be made by EA based on the contractor's ability to meet payment milestones as defined in the Bid Documents in the following manner.

5.5.1 For Supply of Equipment (Hardware & Software);

5.5.1.1 EA will make payment equal to 50% of the amount of equipment on the arrival of Equipment at site of installation and certification by EA Project Director/Manager of their receipt in good condition.

5.5.1.2 Balance 50% of the amount of equipment will be paid on issuance of RFS for the complete system area in individual city.

5.5.2 For Installation, Testing, Commissioning and Professional Services.

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

5.5.2.2 Balance 25% of the amount of Services cost will be made at the time of issuance of final PAC for complete system in individual city.

5.5.3 For System Support and Maintenance Services.

5.5.3.1 EA will make payment on quarterly basis at end of each quarter, after support/service delivered.

7. Penalty:

7.1 If the contractor fails to complete the said job on or before the Completion Date, the Contractor shall pay to the Purchaser as and by way of Penalty resulting from the delay, the aggregate sum of one percent (1%) of Total Contract price of the delayed services for each week and pro-rata for parts of week, for delay beyond the specified date, subject to a maximum of ten percent (10%) of the Total Contract Price of the service(s). In the event that delay is only in respect of small items which do not affect the effective utilization of the system, penalty shall be chargeable only on the value of such delayed items.

7.2 Any penalty chargeable to the Contractor shall be deducted from the invoice amounts submitted by the Contractor for payment, without prejudice to the Purchaser’s rights.

8. Construction of Contract:

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

9. Termination of the Contract

9.1 If during the course of the Contract, the Contractor shall be in breach of the

Contract and the Purchaser shall so inform the Contractor by notice in writing, and should the breach continue for more than seven days (or such longer period as may be specified by the Purchaser) after such notice then the Purchaser may immediately terminate the Contract by notice in writing to the Contractor.

9.2 Upon termination of the Contract the Purchaser may at his option continue work either by himself or by sub-contracting to a third party. The Contractor shall if so required by the Purchaser within 14 days of the date of termination assign to the Purchaser without payment the benefit to any agreement for services and/or the execution of any work for the purposes of this Contract. In the event of the services/jobs being completed and ready for utilization by the Purchaser or a third party and the total cost incurred by the Purchaser in so completing the required services/jobs being greater than which would have been incurred had the Contract not been terminated then the Contractor shall pay such excess to the Purchaser.

9.3 The Contractor shall not have the right to terminate or abandon the Contract except for reasons of force majeure.
9.4 Etisalat has the right to terminate this Contract without cause at any time by serving a 30-day prior written notice to the Contractor.

10. Local Taxes, Dues and Levies:

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

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

Annexure-A

Part A: (Scope of Work)

1. HIGH LEVEL

- Etisalat Afghanistan is looking to swap/upgrade its existing ADMS (Automatic Device Management System) to a new advanced version to fulfill the new technical and commercial demands of the market.
- The bidder shall undertake the complete implementation of the new ADMS end to end.
- The new ADMS shall be capable of providing API for all types of Automatic device Management systems from devices detection through Core Network (CS & PS) to CRM, CVM, DWH and any other systems that needs ADMS triggers for device-based campaigns or events.
- The bidder shall propose the bid for two options for the upgrade, with HW and without HW. In the case of without HW, the bidder shall share the required BoM with Etisalat Afghanistan (EA).
- The bidder/contractor shall submit a weekly progress report identifying the progress to date about the current plan of work, specifying areas where remedial actions may be required to maintain the current plan of work stating clearly whether the planned completion date will be achieved or will be revised to a new planned date in case of major delay.
- The bidder/contractor shall assign adequate and necessary manpower (Project Manager, Technical engineers) dedicated to this project to fulfil the implementation requirements.
- The above-mentioned Engineering Support staff will be fully dedicated to the project and will not be assigned any unrelated tasks by the Contractor.

2. AUTOMATIC DEVICE MANAGEMENT SYSTEM GENERAL FEATURES.

- ADMs System Detection for GSMA & Non GSMA Devices.
- User Management
- Monitoring
- Greetings Messages,
- Device Repository
- Subscribers Information
- Marketing
- Broadcast
- Custom Features
- SIM OTA
- Dashboard for all types of Devices graphical statistic.
- Pre-defined Reports included of
  - Device Distribution,
  - Device Configuration,
  - Traffic Statistics,
  - Subscribers Lists,
- License Counter,
  - Number of detected subscribers,
  - Number of configured handsets,
  - Number of purchased licenses.
- KPI, CDR, Logs storing and backup.
- Evolution Charts;

  - Evolution of a specific handset capability i.e. LTE, VoLTE, RCS, NFC, IPV6, NITZ, MMS, WAP, EMAIL, GPS, CAMERA, Video Calling, JAVA, WLAN, HD Voice and Dual SIM
  - Evolution of a specific device model
  - Evolution of a specific manufacturer
  - Evolution of a specific data technology i.e. GPRS, EDGE, 3G, HSPA, HSPA+, DC-HSPA, LTE and Advanced LTE
  - Evolution of a specific OS Platform
  - Trends by OS Platform
  - Trends by Device Type
  - Trends by Data Enabled Devices
  - Trends by Manufacturer
  - OS transitions
  - Manufacturer Transitions
- Fraud Reports;
  - List of Unknown TACs
  - Percentage of Unknown TACs
  - Number of Unknown TACs
  - New Detected IMEIs
  - Device distribution per GSMA certified devices
  - Top Repeated IMEIs
- Handset Change;
  - Top 50 OTA Subscribers
  - Average Device Holding Time
  - Handset Change Report

- Custom Reports:
  - “Device Distribution” (pie/bar chart) showing the percentages.
  - “Subscribers lists” that can be downloaded showing the “Model, IMSI, MSISDN, IMEI, OS, DEVICE TYPE, Activation Date.”
  - “Detected TACs” list that can be downloaded showing the “TAC, Model, OS, DEVICE TYPE”
  - Subscribers Count

- Device Attributes
- SIM Advertisement Related Features
- Support of WIB
- STK SIM Advertisement Applet
- S@T Support
- Bulk Campaign Management
- Blacklisting Subscribers
- Subscribers Segmentation
- Geo-Fencing
- Time-Fencing
- Limitation Rules per Subscriber
- Limitation Rules per Channel
- Advanced Limitation Rules
- Control Group
- SIM Advertisement Contents
- Information and Promotional Services
- Subscription Enabling

- Customer Surveys
- Interactive Menus
- Mobile Advertisers
- Event Based Notifications
- Reminder Notification
- External Integrations
- Developer APIs
- Integration with Provisioning Node
- Integration with Charging Node
- Administration Related Features
- General Statistics
- Administration Interface
- Network Triggered Purge
- Technical Pre-Requisites
- Use Cases
- External Promotional Contents
- Balance Top-up
- Customer Feedback on LTE Speed
- SIM Advertisement on Call Termination
- Location Based Advertisement
- Financial Services
- Solution Architecture
- Platform Hosting
- Software Modules
- Network Integration

- Supported SIM cards.
- SPN Change Support
- Triplet (IMEI, MSISDN, IMSI) blacklisting in GUI.
- Manual OTA Setting pushing.
- Setting Campaign via SMS.
- eSIMs device detections.

3. SYSTEM CAPABILITIES:

- Capability to connect with MSC.
- Capability to connect with Billing interface MML.
- Capability to connect with SIGTRAN.
- Capability to connect with NTP.
- Capability to connect with SNMP.
- Capability to connect with Mediation through SFTP and EDWH for OTA Dump
- Capability to connect with SGSN/GGSN
- Capability to connect with STP.
- Capability of API connectivity
- Capability to connect with HLR.
- Capability to support HTTPS for web URLs.
- Capability of IMS for the VOLTE.
- Capability of Devices detection per CELL Base.
- Capability of Triplet (IMEI, MSISDN, IMSI)
- Capability of SMSC Connectivity for OTA Setting Delivery.

4.

5. COMMERCIAL REQUIREMENTS

- OTA system should have integration capabilities to pick tags related to service provisioning tag in Billing.
- OTA system should confirm the accurate handset type(2G/3G/4G) as per GSMA standards(Unlike the current system, where the handset type is captured blank for ~25% handsets)
- Missing Handsets in OTA dump as compared to 90-day base(In the current system ~5% of the 90 day base doesn't feature in OTA base. The proposed OTA system should eliminate this scenario)
- OTA system should have integration capabilities with Billing to check Usage against technology and then cross check with the GSMA tag(For example, if the customers use 3G technology and OTA tag is 2G, the same should be highlighted)
- OTA system should map the tower technology (as per the max cell ID) as well against the MSISDN.
- OTA reports should provide insights on device migration trends etc/ province wise trends etc

6. DOCUMENTATION and TRAINING

- The bidder/contractor undertakes to provide adequate numbers of complete Documentation including Operations, Maintenance & Service manual for the ADMs platform.
    - ADM Features Descriptions
    - ADM CDRs Format Description
    - ADM Marketing Tool Features
    - ADM Operation and Maintenance Manual
    - ADM Service Device Repository
    - ADM Service Key Performance Indicators

- ADM SIM Control SIM Advertisement Service Description

- Unless otherwise specified by Etisalat-Afghanistan, all documentations shall be in the English Language.
- The documentation shall be supplied by the Contractor for all elements of the system as per the General specifications of the tender and contractor's compliance which forms integral part of this contract and shall be valid for both contracted equipment (including third party equipment) supplied as part of the contracted System.
- The bidder shall consider 5 days class-based training for EA's technical staff.

7. **DELIEVERY METHOD:** In the case of the HW Delivery on bidder/contractor, the bidder/contractor should deliver ADMS equipment to Afghanistan CIP or DDP based.
8. **INFRASTRUCTURE (VIRTUALIZED BASED):** The system and software shall be compatible with the Virtualized based infrastructure. In case EA's is providing the infrastructure, the contractor shall share the full details in the BoM related to disk space, memory, CPU, storage and overall VMs dimensioning.
9. **AUTOMATIC FAILOVER:** The system shall have automated mechanism of both in Hardware and Software levels for failovers to ensure the service availability and business continuity.

10. **BACKUP AND RESTORATION:** The system should come with the capability to backup configurations and based on EA's requirement, and restoration to happen when needed without any issues.

11. **SYSTEM REDUNDANCY AND RELIABILITY**

- The contracted equipment shall be fully redundant to provide a very high degree of availability (99.99%). should have built-in redundancy and failover mechanism to ensure high availability.
- Load Balancing: should employ load balancing techniques to distribute traffic evenly across multiple servers or nodes.

- The system should have redundant network connectivity, utilizing multiple network links or carriers to ensure continuous communication and minimize the impact of network outages or disruptions.
- The system shall provide remote testing, integration, and software upgrade for all the contracted system elements from the OSS, which can be carried out without the requirements of a visit to the site.
- Monitoring and Alerting: should include robust monitoring capabilities to track system performance, health, and availability in real-time.
- Regular Maintenance and Updates: should have a documented maintenance and update schedule for the ADMS system, including patch management, security updates, and firmware upgrades.
- The system shall provide an external drive, which will be used for an external backup. The following type of backup shall be provided by the system.
- System backup including the operating system, database, and log file.
- Alarm, events, and statistics backup.

12. SYSTEM PERFORMANCE

- The Contractor shall be responsible for any degradation caused by the performance of the contracted equipment or any of its part (Hardware, Software, Application, Database, and Operating System). Hence, the Contractor shall provide full solution for any degradation at no additional cost to Etisalat-Afghanistan, within one month of the date of first appearance of the problem.

13. INTERFACES & INTEROPERABILITY:

- The Contractor shall guarantee full compatibility and interoperability of the supplied equipment with Etisalat-Afghanistan existing / concurrent multi-vendor equipment with standard interface, infrastructure, and GSM,3G,4G, IMS/VoLTE & IOT 5G Network, which are compliant with the GSM and 3GPP standards.
- The contracted System shall support integration with multi-vendor equipment with standard interface and API based.

- The contracted System shall integrate easily and efficiently with Etisalat-Afghanistan existing / concurrent infrastructure.

14. SOFTWARE RELEASES/FEATURES & UPGRADE

- The contracted System shall be scalable and upgradeable to support future growth of subscribers, new resource intensive applications and shall comply with future GSM specifications, services, and enhanced features.
- Any planned system HW/SW upgrades shall be implemented with minimum service interruption.
- The contracted System shall be modular and expandable both in capacity and in services / features.
- The Contractor shall provide, at no additional cost, all hardware, software, and additional development that are found necessary for implementing those features into the contracted ADMs equipment.
- Software support and modifications considered necessary by Etisalat-Afghanistan due to the design defects/bugs either with the operating system of/or related to the applications shall be guaranteed for the life span of the equipment. The Contractor shall notify Etisalat-Afghanistan immediately on identification of the effect and shall arrange to effect immediate correction. The correction notification shall be made known to Etisalat-Afghanistan prior to the installation of the correction to enable smooth transition/correction of the bugs/design defects.
- All features available in the current SW Release shall be included in the upgrade (besides the new features available to the upgrade SW Release) and all features available in upgrade SW Release shall be included in the next SW Release and henceforth.
- The Final Acceptance Certificate (FAC) shall be issued upon the successful implementation of the latest Software Release in all the contracted network elements. In the event of delay in implementing the latest SW release, the duration of the delay shall be added as an extended warranty over and above the agreed warranty period for the System.

- The Contractor immediately upon its availability shall provide all new Software Releases features list.

15. TESTING AND DEBUGGING

- The Contractor shall, jointly with Etisalat-Afghanistan, conduct tests on the Hardware and Software installed. The Contractor shall also remove any bugs/ discrepancies and replace/ vulnerabilities/ modify the defective hardware, software, application components, and re-run the acceptance tests again until all the tests are successfully concluded.

16. CYBERSECURITY:

- Etisalat Afghanistan will be committed to secure better the hardware and software machines with no risk or attack to protect and need to be installed EA IT Tool Securities in EA Automatic Device Management Servers, Applications, SSL certificates required to be applied for local or public URLs.
- In case of any scanning and online session need the contractor to be available 24/7 to trouble shoot high and vulnerabilities to be remediated immediately from any risks
- The system should support the Cybersecurity tools including but not limited to S1and NESSUS.
- The system should support integration with Cybersecurity systems including but not limited to Signalling FW, SIEM, IAM, PAM and NAC.
- The system shall support authorization, access control and security reporting functions.
- The system shall be able to create a flexible access profile for each user, which will allocate an access to specific task in the system.
- The security shall provide the following main access categories:
    - System super user (root)
    - Application administrator
    - Database administrator
    - Normal User

    - Other required roles availability

- The bidder/contractor must ensure their operating systems are up to date and is not End of Life/End of Support.
- The bidder/contractor must ensure proper patch management of their servers in alignment with EA IT and Cybersecurity policies.
- The bidder/contractor must ensure a licenses and standard AV solution is installed in all their operating systems.
- The bidder/contractor must ensure full cooperation and coordination with EA SOC "Security Operations Center" team whenever required and deemed appropriate.
- The bidder/contractor must not install any application without proper coordination and agreement of EA SOC Team.
- The use of insecure cryptographic algorithms and protocols are strictly prohibited, and all integrations and system communication must be based on secure and strong cryptographic algorithms.
- The bidder/contractor must ensure strong protection of EA data stored on vendor's cloud.
- EA's data stored on vendor cloud must be destroyed whenever required and requested by EA.
- The bidder/contractor must align all of their services and configurations in accordance to EA Information Security policies and standards.
- The bidder/contractor must use and install only licensed applications.
- The installation and Integration of servers must be aligned with IT requirements.
- The bidder/contractor must not use/install any application/service that is not required.
- The bidder/contractor must communicate any software installation with EA SOC team and get approval.
- The bidder/contractor must align their changes according to EA Change Management Policy.

- The bidder/contractor must ensure all their operating systems are fully patched with the latest OS/Software updates.
- The bidder/contractor must not use any OS that is/will be End of Life / End of Support in less than 1 year.

17. WARRANTY PERIOD

- The Contracted System including all its components shall be covered by warranty throughout the implementation period(s) and for a period of twelve (12) calendar months, commencing from the date of issuance of the Provisional Acceptance Certificate (PAC) by Etisalat Afghanistan.
- All new major releases and minor update revisions for any of the supplied software components, as and when these are issued for general deployment, shall be provided free of charge during the warranty period.
- The Contractor at no cost to Etisalat Afghanistan shall replace any unit or component, which fails during the installation/warranty period.
- The Contractor undertakes to provide Etisalat Afghanistan, full Warranty Support Services by qualified Engineer(s) based in Afghanistan for the complete contracted System / Network, during the entire implementation and warranty period, within the contracted cost. If there exist unresolved snags and problems with the contracted System at the end of the warranty period and which affects the System performance / functionality, then the warranty Support shall be extended by the Contractor at no additional costs, until such snags are resolved to the satisfaction of Etisalat-Afghanistan. Such engineer(s) shall provide within a reasonable time solutions to problems, clearing of system faults and answers to technical questions concerning the supplied equipment. This service will be offered at no cost to Etisalat-Afghanistan.
    - The Contractor undertakes the responsibility of providing Technical Support Service to Etisalat-Afghanistan by qualified Technical Support staff based in Afghanistan, during the entire warranty period of the System. Such Technical Support staff shall be capable to provide solution to problems, clearing of

system faults and answers to technical questions concerning the supplied equipment within reasonable time limits.

- In addition to local technical support, "tele-assistance" from Contractor's nominated support office shall also be available on 365/366 days of the year on 24 hours basis, at no additional cost to Etisalat-Afghanistan during the entire warranty period.
- In addition to the above, according to agreed SLA, the Contractor shall resolve all faults reported in writing by Etisalat-Afghanistan within a time frame.
- The Contractor shall make available compatible replacement spares and proprietary components for a period of 15 years for the contractor products or 3rd party products.
- If the performance of the Contractor's Engineering Support staff is not found standard, the Contractor shall provide a replacement within four weeks from the date of such notification by Etisalat-Afghanistan.

18. REPAIRS / REPLACEMENT OF FAULTY UNITS

16.1 Replacements under Warranty:

- In case the HW is provided by the Contractor, the Contractor at no cost to Etisalat-Afghanistan shall replace any unit or component, which fails during the installation/warranty period.
- The Contractor shall make provision of sufficient spare equipment in the Contractor's local offices in Afghanistan so that any faulty equipment can be replaced immediately (within 6 hours) from the time of the first notification made by Etisalat-Afghanistan or the time when fault has become apparent.
- Etisalat-Afghanistan stock of spares shall not be utilized during warranty for replacements.
- A fault report shall be provided for each repaired unit.

- The Contractor shall provide every month a statistical report covering all types of faulty units/sub-units.
- Equipment is repaired or replaced (during warranty) by the Contractor shall be warranted for the remainder of the original warranty period or twelve (12) months from the date of replacement, whichever is longer. Date of repair shall be clearly inscribed on such units.

19. MAINTENANCE & SUPPORT SERVICES:

- The contractor shall be responsible for Network Operation& Maintenance services and Network Planning& Optimization services, from the date of issuing the RFS and continue without any extra cost.

20. SLA – SERVICE LEVEL AGREEMENT:

EA is committed to having a highly available service to its customers so the ADMS providing OTA as a basic service should support high availability. Accordingly, the contractor must take full responsibility on the Service Level Agreement as mentioned below:

	Severity		
	Critical	Major	Minor
	The entire system is down. OR Key application is down	Part of the system is down. OR Degraded performance OR Incorrect behavior in key application	Faults which do not result in downtime of system or application. OR UI issues
Response Time	15 minutes	30 minutes	90 minutes

Tech Support (24*7) Services Availability	24/7	24/7	8/5
Time to recover service to operational condition. (For software issues)	90% within 4 hours 100% within 6 hours	90% within 8 hours 98% within 24 hours	On best effort basis
Time to Recover service. (For hardware issues)	Within 48 hours on best effort basis	Within 96 hours on a best-effort basis	On best effort basis

21. SPARE PARTS

- In case the HW is provided by the Contractor, the Contractor shall guarantee the availability of spare components, units, sub-units, compatible equipment's, and replacement parts, for the System, for a period of minimum 5 years for contractor Products and the same for third party Products, from the date of the Final Acceptance Certificate of the last order.
- In case of technology change, prior nine months' notice shall be given to Etisalat Afghanistan in order to examine the feasibility of bulk procurement of such parts.

All spares provided and/or that will be provided under this Contract shall have a warranty of 12 months starting from the date of receipt at The Contractor's warehouse. The date of manufacture shall be clearly indicated on the spares. The printed circuit boards/equipment shall not be manufactured earlier than six months from the date of delivery; otherwise, the additional period over and above the six months will be added to the period of the original warranty to define the actual warranty period of the unit.

Annexure-B

Cybersecurity Requirements

General Security Requirements:

1. Vendor must ensure their operating systems are up to date and is not End of Life/End of Support.
2. Vendor must ensure proper patch management of their servers in alignment with EA IT and Cybersecurity policies.
3. Vendor must ensure a licensed and standard AV solution is installed in all of their operating systems.
4. Vendor must ensure full cooperation and coordination with EA Cybersecurity team whenever required.
5. Vendor must not install any application without proper coordination and agreement of EA SOC Team.
6. The use of insecure cryptographic algorithms and protocols are strictly prohibited and all integrations and system communication must be based on secure and strong cryptographic algorithms.
7. Vendor must ensure strong protection of EA data stored on vendor's cloud.
8. Vendor must align all of their services and configurations in accordance to EA Information Security policies and standards.
9. Vendor must use and install only licensed applications.
10. The installation and Integration of servers must be aligned with IT and Cybersecurity requirements.
11. Vendor must not use/install any application/service that is not required.
12. Vendor must communicate any software installation with EA Cybersecurity team in advance.
13. Vendor must align their changes according to EA Change Management Policy.
14. Vendor must ensure all their operating systems are fully patched with the latest OS/Software updates.

15. Vendor must not use any OS that is/will be End of Life / End of Support in less than 3 year.
16. Only secure and strong cryptographic algorithms are allowed to be used in the vendor platforms.
17. System must support Role Based Access Control, and Rule Based Access Control
18. System must provide Strong authentication and authorization mechanisms
19. System must be capable of advanced logging mechanisms to ensure user activities are logged for audit and security purposes and the log must include all of the following at minimum.
    - Failed and successful logins
    - Modification of security settings
    - Privileged use or escalation of privileges
    - System events
    - Modification of system-level objects
    - Session activity
    - Account management activities including password changes, account creation, modification…
    - Event logs must contain the following details:
    - Date and time of activity
    - Source and Destination IP for the related activity
    - Identification of user performing activity
    - Description of an attempted or completed activity.
20. The system must support live log retention of 1 Year and backup up to 3 years.
21. System must be capable of encrypting the log files to ensure user does not modify or change the logs.
22. System must provide cryptographic algorithms such as AES 128/256 Bit, SHA 256/384/512 bits.
23. System must be secure against well-known attacks including but not limited to SQL Injection, XSS, CSRF, SSRF, Code Execution and other attacks.
24. Vendor system's password configuration must be aligned with EA Information security policies.

25. System must support integration with LDAP, IAM "Identity and Access Management" and PAM "Privileged Access Management" Solutions.
26. System must support external log synchronization mechanisms to push logs to another system for analysis such as SIEM and centralized log server.
27. The database must support the encryption of admin user's information with algorithms such as PBKDF2 and SHA256/384/512 bits.
28. The database platforms "if any" must support the encryption of data in-transit and at rest.

Important Note:

Bidders, vendors, and any concerned party shall fill all the fields in the below table, any missing or non-compliant item may cause disqualifying the proposed system from the Etisalat Security side.

No.	**Description**	**Compliance (YES/NO/NA)**	**Comments**
1	**Etisalat Security Requirements**		
1.1	The Contractor/Supplier/vendor to sign Non-Disclosure Agreement (NDA) with Etisalat before finalizing RFx/contract/POC agreement as per Etisalat NDA process.		
1.2	Contractor/Supplier/vendor equipment's (e.g. Servers, PCs, etc.) that are connected to Etisalat network must be securely wiped before taking out of Etisalat premises.		
1.3	The proposed/contracted system shall pass Etisalat Security Audit (Vulnerability Assessment/Penetration Testing) before go-live/service acceptance by Etisalat. Contractor/Supplier/vendor shall provide SLA for fixing Security gaps based on severity.		
1.4	Contractor/Supplier/vendor shall fix all security issues identified and reported by ETISALAT and/or		

No.	Description	Compliance (YES/NO/NA)	Comments
	Third Party Contracted to do the testing, with no additional cost		
1.5	Contractor/Supplier/vendor confirms that its products/solution are tested for weaknesses via methods such as Vulnerability Assessment, penetration testing, red teaming exercises and scans that check for compliance against the baseline security standards or security best practices, before the new product or any of its releases is delivered to ETISALAT. The Contractor/Supplier/vendor shall provide evidence/report of the security assessment/audit of the proposed solution.		
2	**Security Architecture**		
2.1	The Contractor/Supplier/vendor shall ensure that proposed solution shall comply with the applicable IT and Telecom Security standards (such as Afg. NESA (SIA) IA V2, Afg. DESC (ISR), Afg. TRA, 3GPP, ETSI, ENISA, CSA, NIST, PCI, ISO, GDPR etc.) The Contractor/Supplier/vendor shall confirm the applicable standard.		
2.2	The proposed solution shall support the latest operating systems and application versions. Contractor/Supplier/vendor to ensure proposed solutions will run the latest stable software, operating system, and firmware.		
2.3	The solution shall be designed with multi-tier architecture, (Demilitarized Zone (DMZ), middleware, and private network). Any system accessible from the Internet shall be on the DMZ		

No.	Description	Compliance (YES/NO/NA)	Comments
	and access to internal sensitive data shall be secured through the middle tier application proxy.		
2.4	The proposed solution shall not impact or relax existing Etisalat security control or posture.		
2.5	The performance of the proposed system shall meet the business requirements without disabling or removing any existing security control		
2.6	The Contractor/Supplier/vendor shall provide only secure methods of communication such as HTTPS, SFTP, SCP, TLS1.3, IPSEC, SRTP, SSH v2, SNMPv3 between the proposed nodes. Non-secure protocols such as Telnet, HTTP and FTP shall not be used.		
3	**Password Security**		
3.1	All Operating Systems (e.g. Linux and Windows) shall be hardened according to well-known standards such as, but not limited to NIST, CIS security benchmark, and NSA.		
3.2	The proposed system includes password management module that supports the following features:		
3.3	Setting the minimum password length		
3.4	Password complexity, and not accepting blank passwords		
3.5	Maximum password age and password history		
3.6	Account lockout		
3.7	Enforce changing password after first login		
3.8	Prompt / notify for the old password on password changes		
3.9	The password shall be saved in hashed format (i.e. irreversible encryption)		

No.	Description	Compliance (YES/NO/NA)	Comments
3.10	Forgetting or resetting password function shall support using OTP or email for verification		
4	**Authentication**		
4.1	The proposed system shall not provide access without valid username and password.		
4.2	All user access to the proposed system shall support Privilege account Management (PAM) integration.		
4.3	For public web applications, the proposed system supports and uses CAPTCHA or OTP to prevent password dictionary attacks		
4.4	For mobile applications, the proposed system shall support and uses fingerprint authentication method		
4.5	The proposed system supports and uses secure authentication protocols, like Kerberos, LDAP-S, NTLM V2 and above, HTTPs (for web applications)		
4.6	The proposed system will not use insecure authentication protocols, like NTLM v1, HTTP (for web applications)		
4.7	The proposed system shall support session timeout settings		
4.8	The proposed solution shall support secure API architecture to integrate systems to exchange data where deemed necessary.		
5	**Authorization**		
5.1	The proposed solution shall support role-based access controls that includes access profiles or security matrix (i.e. Role Name VS. Access Permissions)		

No.	Description	Compliance (YES/NO/NA)	Comments
5.2	The proposed system supports role-based access permissions, i.e. Administrator, Operator, Viewer, User…		
6	**Software Security**		
6.1	The software development and testing will not run on the production systems, and will be running in an isolated environment		
6.2	The software source code will not include clear-text passwords		
6.3	The software code will not include insecure protocols, like FTP, telnet …etc.		
6.4	The software testing will not use live/production sensitive or PII data unless it's masked as Etisalat security policy		
6.5	The proposed system enforces input and output validation to prevent security attacks, like SQL Injection, Buffer Overflow…etc.		
6.6	For web portals, the proposed system includes all security controls to prevent/protect from OWASP Top 10 security attacks and risks		
6.7	For mobile application, the proposed system shall include security checks / controls to protect from mobile attacks, like SSL Pinning, Jailbreak, Anti-debug, Anti-hooking, and Advanced Obfuscation…		

No.	Description	Complianc e (YES/NO/ NA)	Comments
7	**Security Event Logging**		
7.1	Proposed systems shall support standard logging protocols such as CIFS/Syslog/CSV logs files		
7.2	The system shall generate and support audit logs that contain the following fields (as a minimum): a) Username b) Timestamp (Date & Time). c) Client IP Address d) Transaction ID & session information		
7.3	The proposed solution shall support the integration with Etisalat NTP for time synchronization and accurate logging.		
8	**Public Cloud Security**		
8.1	Etisalat customers' and staff personal data (PII: name, contacts, address, Emirates ID, Passport number, Nationality ...) is encrypted at rest and in transit using a strong industry-standard encryption protocol		
8.2	The Public Cloud setup that stores PII information shall be hosted in the Afghanistan		
8.3	The Public Cloud setup is hosted in a dedicated tenant for Etisalat (i.e. not shared)		
8.4	The Public Cloud data Center shall not be moved to another country or location without prior coordination and approval from Etisalat		
8.5	All Etisalat data will be permanently erased from the Public Cloud on termination of the service or		

	support agreement		
8.6	The proposed Cloud system supports Etisalat Cloud Access Security Broker (such as Microsoft MCAS, Netskope CASB)		
9	**Virtualization and Container Security**		
9.1	If applicable, Bidder shall ensure the proposed virtualized infrastructure, service based and micro services architecture to support multi tenancy, zoning & micro-segmentation, security visibility, secure virtualization (sVirt), trusted image signing, virtual Firewalls, DoS protection, Trusted platform module (TPM), Hypervisor & Host OS security to secure data and resources.		
9.2	The proposed solution shall support integration with Etisalat/Leading Container Security Solution, where applicable, to scan the container images and ensure malware protection of CI/CD pipeline.		
9.3	Suppliers must inform EA Cybersecurity of any non-conformity with defined EA policies and processes that are agreed upon in advance to acquire a written approval from EA Cybersecurity Department or senior management as required otherwise Supplier will be responsible for all the potential losses		

RFP General Terms Compliance to be filled by Bidder.

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

The following Information must be submitted with offer.

Bidder Contact Details	
Bidder Name	
Bidder Address	
Bidder Email Address	
Bidder Phone Number	
Bidder Contact Person Name	
Bidder Contact Person Phone No	
Bidder Contact Person Email Address	
Bidder Registration License Number	
License Validity	
TIN Number /Tax Number	

================ end of documents ================