TENDER NOTICE

No. EA/02-40-2025

RFP for Onboarding API GW Provider

1. Etisalat Afghanistan invites bids from authorized and qualified providers for the Onboarding API GW Provider, as detailed in the RFP Annexure.

The Bid Document is also available for download on the Etisalat Afghanistan website at: www.etisalat.af/en/about-us/doing-business-with-us/tenders

2. RFP deadline is **15 August 2025 Afghanistan time**.

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

4. Bidders can provide either a sealed Hardcopy of the Proposal or a Softcopy of the Proposal through email. A hard copy can be submitted to Etisalat's Main office, Reception Desk (Tender Box). The softcopy shall be submitted through email (ashalizi@etisalat.af) and cc: (Ihsanullah@etisalat.af and marked clearly with the **RFP name, and number.**

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

6. Etisalat Afghanistan reserves the right to accept or reject any or all bids and to annul the bidding process at any time, without thereby incurring any liability to the affected bidder(s) or any obligations to inform the affected bidder(s) of the grounds for Etisalat Afghanistan action.

7. if you have any questions, you can share them with the below emails:

Name: Ahmad Shikib Shalizi

Title: Assistant Manager of Procurement and Contracts

Email: Ashalizi@etisalat.af

Phone: +93781204040

Ihsanullah Zirak

Director Procurement and Supply Chain

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

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

(RFP)

For

Onboarding API GW Provider

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 Supplier 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 Supplier 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 Supplier and comprising documents.

"Supplier" 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.

"Supplier's Representative" means the person nominated by the Supplier 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 Supplier 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.

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

"Etisalat Afghanistan (EA)" means the company registered under the Laws of Islamic Emirate of Afghanistan and having office at Ihsan Plaza Charahi Shaheed Kabul in person or any person dully authorised by it for the specific purpose for the specific task within the Contract and notified to Supplier 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 Supplier's and EA's control.

"Liquidated Damages" mean the monetary damages imposed upon the Supplier and the money payable to EA by the Supplier 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.

"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 Supplier" for a consortium.

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

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

2. INTRODUCTION TO WORK.

2.1 Bids are invited for the Onboarding API GW Provider in accordance with the stated specifications of RFP documents.

2.2 The tender award will be based on the best technical and price-wise, lowest offer.

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. Suppliers: Responsibilities:

4.1 Supplier shall provide project as described in the RFP scope of work**.**

4.2 Supplier shall have all licenses, permits, and permission required for the provision of this tender.

5. Payment Terms

5.1 All payments shall be made via bank transfer upon receipt of the original hardcopy of the invoice.

5.2 No advance payments shall be made to the Supplier.

5.4 EA commits to making prompt payments within thirty (30) days of the submission of a valid invoice or payment claim by the Supplier. This is contingent upon the receipt of all required supporting documents as specified in the contract and any necessary deductions due to penalties, such as late delivery or the replacement of defective goods, confirmed by the Project Director.

5.5 All payments are subject to the applicable income tax deductions at the prevailing rates, in accordance with the relevant tax laws. These deductions will be remitted to the appropriate tax authorities unless the Supplier is explicitly exempted. EA shall provide a tax deduction certificate to the Supplier to facilitate tax return filings with the relevant authorities.

5.6 All prices and payments shall be made in Afghani (AFN) for local firms and International firms can provide in USD/AFN.

5.7 EA reserves the right to process Purchase Order (PO) or contract-related payments through the mHawala (mobile financial services) platform, directly to the Supplier's registered mHawala account.

6. Price:

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.

6.1 For Supply of Equipment (Hardware & Software);

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.

6.2 For Installation, Testing, Commissioning and Professional Services

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

6.2.2 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.

6.3 For System Support and Maintenance Services (if available).

5.3.1 EA will make payment on quarterly/monthly basis at end of each quarter/month, after support/service is delivered.

7. Local Taxes, Dues and Levies:

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

7.2 Withholding tax (if applicable) shall be deducted on the local portion only as per prevailing rates as notified Islamic Emirate of Afghanistan. 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/ nonregistered companies.

8. Construction of Contract:

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

9. Termination of the Contract

9.1 If during the course of the Contract, the Supplier shall be in breach of the Contract and the Purchaser shall so inform the Supplier 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 Supplier.

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 Supplier 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 Supplier shall pay such excess to the Purchaser.

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

10. Amendment.

No amendment or other variation of the Contract shall be effective unless it is in writing, is dated, expressly refers to the Contract, and is agreed in writing duly signed by authorized representative of each party.

11 AFFIRMATION.

11.1 No Staff or employee of EA shall be admitted to any share or part of this Contract or to any benefit that may arise there from.

11.2 The Supplier declares and affirms that;

A. The Supplier and its shareholders, directors, officers, employees, and agents have not paid nor undertaken to pay, any bribe, pay-off, kick-back or unlawful commission. The Supplier and its shareholders, directors, officers, employees, and agents have not in any way or manner paid any sums, whether in Afghanis or a foreign currency and whether in Afghanistan or abroad, given or offered to give any such gifts and presents in Afghanistan or abroad, to any staff or employee of EA or any other person to procure this tender/contract. The Supplier undertakes not to engage in any of these or similar acts during the term of this Contract.

B. The contract shall be liable for cancellation during any time of execution if such an act is proved.

12. CONFIDENTIALITY OF INFORMATION

12.1 The Supplier shall not, without EA's prior written consent disclose the contract, or any provision thereof, or any specification, plan, drawing, pattern, sample or information furnished by or on behalf of EA in connection therewith, to any person other than a person employed by the Supplier in the performance of the contract. Disclosure to any such employed person shall be made in confidence and shall extend only as far as may be necessary for purposes of such performance.

12.2 The Supplier shall not, without EA's prior written consent, make use of any documents or information except for purposes of performing the contract.

12.3 Any documents, other than the contract itself, shall remain the property of EA and shall be returned (in all copies) to EA on completion of the Supplier's performance under the contract if so required by EA.

13 SUPPLIER'S DEFAULT

13.1 If the Supplier shall neglects to perform the contract with due diligence and expedition or shall refuse/or neglect to comply with any reasonable instructions given to him in writing by EA or any of its authorized representative in connection with the performance of the contract or shall contravene the provisions of the contract, EA may give notice in writing to the Supplier to make good the failure, neglect or contravention complained of.

13.2 Should the Supplier fail to comply with the said notice, within 15 days from the date of issue of said notice thereof, it shall be lawful for EA forthwith to terminate the contract by notice in writing to the Supplier without prejudice to any rights which may have accrued under the contract to either party prior to such termination.

13.3 If EA have to incur extra cost for procuring any part of Goods or any such similar Goods not delivered in accordance with the Contract on the date of such termination, the Supplier shall pay on demand within one month the amount of such extra costs incurred by EA.

13.4 If the Supplier fails to complete any of his obligations within the extended time mutually agreed between the parties under "FORCE MAJEURE" and EA shall have suffered any loss from such failure, EA shall be entitled to deduct from the contract price at the rate of one (01) percent per week of the contract value of the Goods which cannot in consequence of the said failure be put to the use intended for such work for each week between the time fixed in the Contract (except as aforesaid) and the actual date of completion.

14 FORCE MAJEURE.

14.1 The Supplier shall not be liable for forfeiture of its performance security, liquidated damages or termination for default, if and to the extent that, it's delay in performance or other failure to perform its obligations under the contract is the result of an event of Force Majeure.

14.2 If either party is temporarily rendered unable, wholly or in part by Force Majeure to perform its duties or accept performance by the other party under the Contract it is agreed that on such party, giving notice with full particulars in writing of such Force Majeure to the other party within 14 (fourteen) days after the occurrence Expansion such Force Majeure shall be suspended during the continuance of any inability so caused but for no longer& period and such cause shall as far as possible be removed with all reasonable speed. Neither party shall be responsible for delay caused by Force Majeure. The terms "Force Majeure" as used herein shall mean Acts of God, strikes, lockouts or other industrial disturbance, act of public, enemy, war, blockages, insurrections, riots, epidemics, landslides, earthquakes, fires, storms, lightning, flood, washouts, civil disturbances, explosion, Governmental Export/Import Restrictions (to be supported by a letter from the relevant Authority and verified by the Diplomatic Mission in Afghanistan),Government actions/restrictions due to economic and financial hardships, change of priorities and any other cause similar to the kind herein enumerated or of equivalent effect, not within the control of either party and which by the exercise of due care and diligence either party is unable to overcome. The term of this Contract shall be extended for such period of time as may be necessary to complete the work which might have been accomplished but for such suspension. If either party is permanently prevented wholly or in part by Force Majeure for period exceeding 0ne (01) month from performing or accepting performance, the party concerned shall have the right to terminate this contract immediately giving notice with full particulars for such Force Majeure in writing to the other party, and in such event, the other party shall be entitled to compensation for an amount to be fixed by negotiations and mutual agreement.

If a Force Majeure situation arises, the Supplier shall promptly notify EA in writing of such conditions and the cause thereof. Unless otherwise directed by EA in writing, the supplier shall continue to perform its obligations under the contract as far as is reasonably practicable, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.

15 INDEMNIFICATION.

15.1 Supplier shall indemnify and save harmless EA from and against all losses and all claims, demands, payments, suits, actions, recoveries and judgment of every nature and description made and related cost and expenses brought or recovered against the EA related to the work done under this Contract, by reasons of any act, omission to act or status of liability of Supplier or its agents or employees. Supplier agrees to give EA prompt notice of any possible liability.

15.2 If the Supplier is in breach of any obligations under this Contract (or any part of it) to EA or if any other liability is arising (including liability for negligence or breach of statutory duty) then the maximum liability of the Supplier under this contract shall be limited to the Total Contract Price.

15.3 The Supplier shall indemnify EA in respect of all injury or damage to any person or to any property and against all actions, suits, claims, demands, charges and expenses arising in connection herewith which shall be occasioned by the negligence or breach of statutory duty of the Supplier, any sub-Supplier before or after, the whole of the project has been finally accepted.

16 LIQUIDATED DAMAGES.

16.1 If the Supplier fails to deliver any or all of the Goods or perform the Services in accordance with the delivery milestones specified in the Contract, EA, without prejudice to its other remedies under the contract, shall have the right to terminate the contract forthwith or claim liquidated damages.

16.2 The Supplier shall pay to EA as liquidated damages with respect to those delays in delivering milestones as defined in the Bid Documents. For each delayed milestone damages will be charged at one percent (1%) per week of the total value of the Contract up to a maximum of ten percent (10%). Once the maximum is reached, EA shall forthwith terminate the contract.

16.3 The value of all Goods or part supply of Goods made which are incomplete and therefore not utilized by EA in its operations shall also be added for the purpose of liquidated damages. Any liquidated damages if not paid in cash by the Supplier shall be deducted from the invoice(s) submitted by the Supplier. The imposition of liquidated damages upon the Supplier and its payment shall not absolve the Supplier from its obligations to deliver or from any other liabilities or obligations under the contract.

17. GOVERNING LAW AND JURISDICTION

17.1 This Agreement and any Dispute or Claim arising out of or in connection with it or its subject matter or formation (including non-contractual Disputes or Claims) shall be governed by and construed in accordance with the laws of Afghanistan.

17.2 The Parties irrevocably agree that the courts of Afghanistan shall have exclusive jurisdiction to settle any Dispute or Claim that arises out of or in connection with this Agreement or its subject matter or formation (including non-contractual Disputes or Claims).

18. ANNEXURES:

This RFP has the following annexure as part of the RFP.

1. Annexure –A ……. Scope of Work
2. Annexure- B…… Supplier Code of Ethical Conduct.
3. Annexure –C ……. Compliance Clauses.
4. Annexure-D …… Cybersecurity Requirements

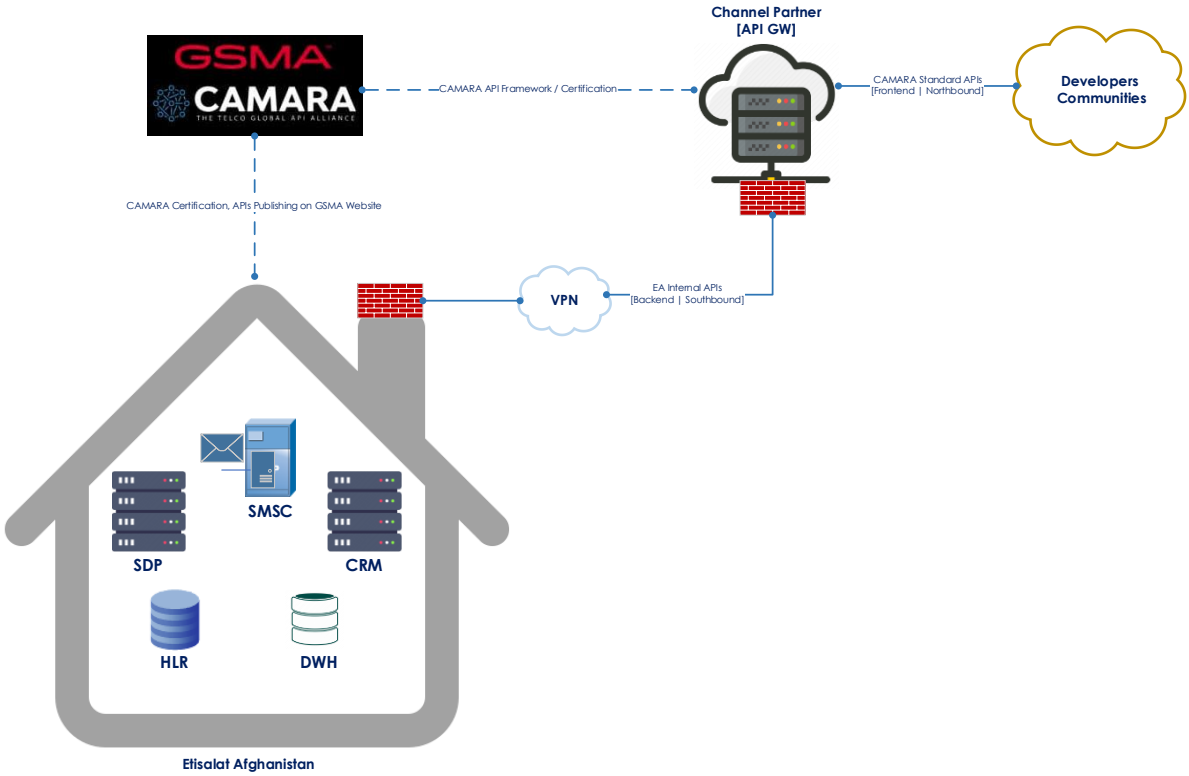
Annexure-A (Scope of Work)

Scope of Work for Onboarding API Gateway Provider for Etisalat Afghanistan

Objective:

The primary objective of this RFP is to onboard an API Gateway provider that will enable the developer community to connect to Etisalat Afghanistan's (EA) network using the GSMA CAMARA APIs. This initiative aims to enhance the accessibility and integration capabilities of Etisalat Afghanistan's network services to the Developers Community and the fulfilment to our commitment to the GSMA Open GW project.

High Level Architecture:



Bidder's Key Responsibilities:

1. **Deployment and Integration:**
    - Define the installation architecture for the API Gateway and whether it is deployable over EA's private cloud or not.
    - Set up the API Gateway to ensure the local integration with EA's internal systems and nodes as well as to be exposed to the external developer's community. This

will apply to traditional Telecom Network Elements such as HLR or VLR or BSS and IT stacks.

- Share a detailed timeline of the implementation (PIP).
- The vendor to submit a **Security Architecture Document**, covering:
  - API Gateway security layers (Northbound/Southbound protection)
  - DMZ placement, reverse proxy usage, and API WAF if applicable
  - Segregation of duties and role-based access enforcement
  - Cloud-specific hardening if deployed on private/public cloud
  - **Zero Trust** Architecture **(ZTA)** principles across all API flows as mandatory.

2. Security Deliverables/Contractual deliverables

- Security Risk Assessment for the API Gateway
- Threat Modeling Report for exposed APIs
- Vulnerability Assessment & Penetration Test (VAPT) results (pre-production)
- Security Hardening Checklist based on CIS (like OS, API Gateway, DB, etc.)
- Audit Logs configuration guide for SOC/SIEM integration
- OWASP API Security Top 10 protections must be implemented (Injection, Broken Auth, Excessive Data Exposure, etc.).
- API Threat Protection (Rate Limiting, Throttling, DoS/DDoS protections).
- Built-in API Schema Validation (OpenAPI / Swagger) to block malformed or malicious API calls.
- Validate input/output sanitization controls.

2.1 Data Privacy and Sovereignty

- Require that all API payloads, logs, and audit trails:

  - Remain within Etisalat Afghanistan's jurisdiction
  - Be encrypted at rest and in transit

- Data Handling for PII, financial, or regulatory data via APIs should be based on Etisalat Afghanistan Cybersecurity Information Classification policy and relevant documents.

- Data Destruction and Retention to be aligned with Etisalat Afghanistan Cybersecurity and IT Policies, and to be aligned with regulatory compliance.

2.2 Secure DevOps (DevSecOps) Integration

Vendor should adopt secure SDLC, and provide:

- Code review logs
- Static/Dynamic security testing results for all developed APIs
- Change control tracking
- Integration with Etisalat's CI/CD pipeline for secure deployment

3. API Management and Maintenance:

- Establish the API Gateway and convert internal APIs for external developer community access based on CAMARA specifications with approximate timelines for each API development.
- Ensure the security and maintenance of the API Gateway and APIs.
- Manage any changes and modifications to the APIs in the future.
- Maintain a readymade Northbound standard APIs of CAMARA that are currently published and the ones coming in the future.
- Assist in certification procedure of EA’s APIs with GSMA/CAMARA.

4. Documentation and Training:

- Provide comprehensive documentation covering installation, upgrades, development, design guidelines, health checks, and troubleshooting.
- Conduct training sessions for EA’s Technical team teams to ensure smooth operation and maintenance of the API Gateway.
- Developer Portal, though which EA team should be able to simulate and troubleshoot existing and new API integrations.

5. Post-Production Support:

- Offer post-production support, including access to a trouble ticket portal and alignment on Service Level Agreements (SLAs) to ensure timely resolution of issues. Further, vulnerability management and Cybersecurity incident management should be based on Etisalat Afghanistan Cybersecurity related policies and documentations.

6. Cybersecurity Compliance:

- Implement stringent cybersecurity measures to secure hardware and software, including the use of tools like following:
  - EDR/XDR
  - HTTPS (TLS 1.2/1.3)
  - Validate input/output (anti-SQLi, XSS)
  - Enforce strict authentication (OAuth 2.0, MFA)
  - Monitor & log API traffic (SIEM integration)
- Provide an extra layer for application and API level security between the Northbound and the Southbound interfaces.
- Support authorization, access control, and security reporting functions, with flexible user access profiles for different roles.

7. Operational and Security Policies:

- Ensure operating systems are up-to-date and supported, with proper patch management in alignment with Etisalat Afghanistan's IT and cybersecurity policies.
- Use licensed software and antivirus solutions and coordinate with the Security Operations Center (SOC) for software installations and changes.
- Avoid insecure cryptographic algorithms and ensure strong protection of data stored on the vendor's cloud, with data destruction upon request.
- Comply with Etisalat Afghanistan's information security and change management policies.

8. Business Model

Share the business model with the details cost breakdown for initial setup, API development efforts and remote maintenance post-delivery.

The following Information must be submitted with the 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	

Contract – Annexure B:

Etisalat Afghanistan's Supplier Code of Ethical Conduct – Making Good Possible Together

Content

1. Supplier Definition and Scope

1.1. The term **Supplier** means any person, entity or organisation that provides or seeks to provide Etisalat Afghanistan with products, goods, or services. This includes all officers, employees, Suppliers, subSuppliers, and agents of any Supplier.

1.2. This Supplier Code of Ethical Conduct applies to all Etisalat Afghanistan Suppliers and their procurement agreements.

2. Purpose of this Code

2.1. **Etisalat Afghanistan** is fully committed to doing business in accordance with the highest standards of ethics and integrity, with professional business principles and in compliance with all applicable laws in the country. We recognise the importance of earning and maintaining the trust of our customers and stakeholders where we operate.

2.2. We expect our Suppliers to abide with this Code (as defined below) and conduct all our business and relationships with the highest standards of ethics to maintain this trust.

2.3. This Supplier Code of Ethical Conduct (**the "Code"**) sets out Suppliers' obligations in relation to compliance with ethical conduct, any relevant legal obligations including anti-bribery and anti-corruption, sanctions, export and trade controls, and relevant regulations and standards in the Country in which the Supplier operates.

2.4. The purpose of the Code is to promote safe working conditions and the responsible management of social, ethical, and environmental issues in Etisalat Afghanistan's procurement and supply chain. This includes issues such as human rights, working practices, labour standards, environmental, the responsible sourcing of minerals and health and safety.

2.5. The Supplier is encouraged to ensure its own Suppliers and subSuppliers are made aware of the principles of the Code when undertaking any work, or providing any product or service to, or on behalf of Etisalat Afghanistan.

3. Supplier selection and on-boarding

3.1. Etisalat Afghanistan is committed to doing business with the highest standards of ethics and integrity. We expect that our partners, Suppliers, consultants, agents, etc. apply the same standards.

3.2. To ensure that Etisalat Afghanistan work with the right third parties and to protect Etisalat Afghanistan's brand and reputation, we conduct a thorough registration/selection, due diligence, and engagement processes prior to on-boarding or engaging any Suppliers.

3.3. The Supplier shall take reasonable steps to ensure that it's selection processes also include adequate due diligence on sub-Suppliers.

3.4. The Supplier shall ensure it does not commence any work or activities on behalf of Etisalat Afghanistan until it confirms it has read, understood, and will comply with all the principles set out in this Code.

4. Supplier monitoring

4.1. The Supplier must ensure they have processes in place to identify, correct and monitor the continued compliance of any activities that fall below the standards of ethical conduct set out in this Code.

4.2. Any breach of this Code may be considered to be a material breach of any agreement or contract with Etisalat Afghanistan, and Etisalat Afghanistan reserves its legal rights and remedies in respect of any such breach.

5. Data Protection, Privacy and Confidentiality

5.1. At Etisalat Afghanistan, we respect the privacy of our customers and third parties, as well as of others with whom we conduct business.

5.2. The Supplier must ensure they handle any confidential or customer personal data with due care, ensuring it has a process in place to ensure access and storage of this data is managed securely.

5.3. The Supplier shall ensure that any authorised communication of Etisalat Afghanistan confidential or customer information should be limited to appropriately trained and authorised individuals who need it to carry out their work, in accordance with applicable laws and for legitimate business purposes only.

5.4. The Supplier must ensure they protect any Etisalat Afghanistan confidential or customer information from improper disclosure.

5.5. The Supplier shall respect Etisalat Afghanistan's brand and intellectual property rights and manage any technology and know-how it receives from Etisalat Afghanistan in a manner that protects these intellectual property rights.

6. Modern Slavery, Child Labour, and Human Trafficking

6.1. Etisalat Afghanistan is committed to ensuring all workers in our procurement & supply chain receive fair and equal treatment in full compliance with the laws, rules, and regulations of the country. In case there are different standards set forth in this Code compared to the applicable laws, rules, and regulations, Etisalat Afghanistan expects the same standards or more stringent requirements to be applied.

6.2. Etisalat Afghanistan prohibits the use forced labour, whether in the form of prison labour, indentured labour, bonded labour or otherwise. No employee or worker may be compelled to work through force or intimidation of any form, or as a means of political coercion. Also, we operate a zero-tolerance policy for any form of Slavery and Human Trafficking in our operations and procurement & supply chain. The Supplier shall not permit the use of any form of forced, bonded, compulsory labour, slavery, or human trafficking. We will treat any reported incidents seriously, with respect and in confidence.

6.3. Etisalat Afghanistan condemns all forms of exploitation of children. We remain committed to prohibit and eliminate the use of child Labour in our operations and procurement & supply chain. Our aim is to ensure that all our operations remain in compliance with national regulations. The Supplier shall not knowingly use any child labour and should not employ or engage anyone who is below the minimum legal age for employment in line with applicable laws in the country.

6.4. All the Supplier's employees shall be freely employed. This means all employees must be provided with employment contracts that stipulate, the employee's rights to terminate their employment with reasonable notice period, the working hours, and the minimum wage and required benefits in line with applicable laws in the country.

6.5. The Supplier may deduct subsistence expenses from employees' wages as required and substantiated for the nature of the work or in accordance with established company policies (Article 95 of Afghanistan's Labor Code). Any such deductions must be transparent, justified, and consistent with reasonable standards, ensuring that they do not impede an employee's basic rights or cause financial hardship. However, the Supplier shall refrain from making any other wage deductions, withholding payments, imposing unauthorized debts upon employees, or demanding the surrender of government-issued identification, passports, or work permits as a condition of their employment. All deductions must comply with fair and legal practices, respecting the rights and protections afforded to employees under the prevailing labor regulations. The Supplier shall not engage in or support the use of corporal punishment, threats of violence or other forms of mental or physical coercion. All employees shall be treated with dignity and in accordance with our policies maintaining a work environment that is free of any sort of physical punishment. All employees should be aware that we will treat all incidents seriously and with respect and in confidence and we will promptly investigate all allegations of physical punishment. No one will be victimized for making such a complaint.

7. Discrimination

7.1. Etisalat Afghanistan believes that everyone should be treated with dignity and respect, therefore, Etisalat Afghanistan prohibits all forms of discrimination, harassment, humiliation, threats of violence and abusive or offensive behaviour.

7.2. The Supplier shall not engage in, or support, any form of discrimination, in hiring, employment terms, remuneration, access to training, promotion, termination, retirement procedures or decisions including but not limited to race, ethnicity, skin colour, age, gender identification or any other characteristics protected by law, pregnancy, disability, religion, political affiliation, nationality, medical condition, social origin, social or marital status and trade union membership.

8. Bribery and Corruption

8.1. Etisalat Afghanistan's stance on avoiding Bribery and Corruption means that regardless of local customs, we never receive or provide Gifts, Entertainment, Hospitality or any other benefits that are motivated by an improper purpose, such as to gain an inappropriate business, personal or other advantage.

8.2. The Supplier shall not tolerate or enter into any form of bribery, including improper offers or payments to or from employees, customers, Suppliers, organisations or individuals.

8.3. The Supplier shall abide by all applicable anti-corruption laws and regulations of Etisalat Afghanistan and applicable laws in the country, including the Foreign Corrupt Practices Act ("FCPA") and applicable international anti-corruption conventions.

8.4. The Supplier shall have an anti-bribery policy that sets out the principle of zero tolerance to any form of bribery or corruption within their organisation, including facilitation payments.

8.5. In the course of doing business with or on behalf Etisalat Afghanistan or fulfilling any agreement or contract with Etisalat Afghanistan, the Supplier must not in relation to any public or government official, offer, give, promise, receive or request any bribes (financial or any other improper advantage).

8.6. The Supplier shall ensure its employees, Suppliers and sub-Suppliers are aware of its antibribery policy and how to comply with its requirements.

9. Money laundering

9.1. The Supplier shall act in accordance with all applicable international standards and laws on fraud and money laundering and (where appropriate) maintain an anti-money laundering compliance programme, designed to ensure compliance with the law including the monitoring of compliance and detection of violations.

10. Health & Safety

10.1. The Supplier shall ensure it provides a safe working environment for employees, Suppliers, partners, or the community who may be affected by Supplier's activities, in accordance with international standards and national laws.

10.2. The Supplier shall ensure it meets general principles of health and safety risk prevention. General principles include ensuring it has systems and processes in place for identifying, minimising, and preventing health and safety hazards, using competent and trained people, providing and maintaining safe equipment and tools, including ensuring personal protective equipment is made available as required.

10.3. The Supplier shall ensure that these health and safety obligations are communicated and applied to all parties including sub-Suppliers when undertaking any work or activities on behalf of Etisalat Afghanistan.

10.4. Suppliers, vendors, and Suppliers carrying out work for & on behalf of Etisalat Afghanistan are obliged to comply with Health, Safety & Environment (HSE) policies, rules, standards, processes, procedures, and best international practices.

10.5. Conform with all the local laws and regulations laid down by the Government of Afghanistan related to their operations, wellbeing, health of employees, public, protection and sustainable use of natural resources and the environment they operate.

10.6. the Suppliers are required to strictly follow and implement mentioned HSE regulation and standards during their operations and activities. The instructions are produced primarily for the use of the Supplier's management and supervisory staff who are required to ensure that the rules and procedures are brought to the notice of all the Suppliers' workers and that such rules and procedures are strictly followed by them.

10.7. EA will not be responsible for any damages, loss, incident, legal issues, and non-compliance with HSE standards that may arise from the Suppliers' activities.

10.8. Supplier must obtain permit for work and report any HSE related incidents such as injury, fatality, death, and non-compliance to Etisalat Afghanistan HSE focal points and via email hse@etisalat.af.

10.9. For more details about Etisalat Afghanistan HSE Policies and regulations, please contact hse@etisalat.af.

11. Environment and Climate Change

11.1. The Supplier shall commit to protecting the environment. Supplier shall minimise its use of finite resources (such as energy, water, and raw materials) and the release of harmful emissions to the environment (including waste, air emissions and discharges to water).

11.2. The Supplier shall seek to improve the environmental performance of the products and services it provides, as well as support those that offer environmental and social benefits to Etisalat Afghanistan's customers.

11.3. The Supplier shall adhere to relevant environmental legislation and international standards in Afghanistan. In cases where specific environmental legislation is not readily evident or enforced within Afghanistan, the Supplier must establish and maintain reasonable practices to manage environmental impacts in accordance with internationally accepted norms and principles. The Supplier shall identify, monitor, and minimize Greenhouse Gas emissions (GHG) and energy consumption from its own operations including CO2 emissions from transportation and travel and support.

12. Speak Up

12.1. The Supplier shall provide an anonymous complaint mechanism for its managers and workers to report workplace grievances and shall take measures to protect whistleblower confidentiality and prohibit retaliation.

12.2. The Supplier shall report any instances of illegal or unethical behaviour or breaches of this Code (in relation to the goods and services being provided to Etisalat Afghanistan) in confidence using the 'Speak Up' contact details below.

12.3. The Supplier shall regularly promote these Etisalat Afghanistan 'Speak Up' contact details to its employees and any agents or subSuppliers working on the Supplier's behalf for Etisalat Afghanistan: via the official Etisalat Afghanistan whistle-blower email eawb@etisalat.af.

ANNEXURE C, (RFP Compliance Clauses):

1. Anti-Bribery Anti-Corruption

1.1 The Supplier represents and warrants on behalf of itself, its directors and employees and any third-party employed and/or retained to act for or on its behalf including, without limitation, agents, Suppliers, sub-Suppliers and professional representatives (**"Representatives"**) (including executive officers and directors of any such Representatives) that:

(a) it complies and will comply with all applicable laws, statutes, and regulations relating to anti-bribery and anti-corruption including but not limited to the UAE Penal Code and to any applicable foreign anti-bribery and anti-corruption laws.

(b) it will not directly or indirectly through a third party, in relation to, in connection with, or arising from the performance of this Agreement give, receive, promise, attempt to give or to receive or in any way facilitate the giving and/or receiving of anything of value to any person for unlawfully of securing an improper advantage for (an advantage that is not legitimately due to) either Party, inducing or influencing any person to take any action or refrain from taking any action to obtain or retain business for either Party, and/or inducing any government or public official to take or to omit to take any decisions unlawfully;

(c) it has and shall maintain in place throughout the term of this Agreement its own adequate policies and procedures that are aligned with the Relevant Requirements, and shall train its own employees on its policies and procedures to ensure compliance with the Relevant Requirements, and will enforce its policies and procedures where appropriate.

(d) it shall immediately and in any case within three (3) days report to Etisalat Afghanistan in writing any actual or suspected violations including any request or demand for any undue financial or other undue advantage of any kind that it receives in connection with the performance of this Agreement; and

(e) following a request from Etisalat Afghanistan, it shall certify to Etisalat Afghanistan in writing and signed by an officer of the Supplier its compliance with this clause and the compliance of all persons associated with it as well as that of its third parties under this Agreement. The Supplier shall provide such supporting evidence of compliance as Etisalat Afghanistan may reasonably request.

2.1 "Conflict of Interest" shall mean any circumstance, potential, actual, or perceived, that might cause a Party, persons associated with it, or a third party, to place their financial or personal interests above the interests of their contractual commitments and the performance of their obligations under this Agreement causing them to be biased in their business judgments, or to not act in good faith when taking decisions and actions that are detrimental to the interests of the other Party under this Agreement;

2.1.1 The Supplier shall immediately and in any case within three (3) days notify Etisalat Afghanistan in writing if a Public Official[1] becomes an officer or employee of the Supplier or acquires a direct or indirect interest in the Supplier and the Supplier warrants that it has no Public Officials as direct or indirect owners, officers or employees as of the date of this Agreement.

2.1.2 The Supplier represents and warrants that neither it nor any persons associated with it or any third party has interests that would conflict in any way with the performance of its obligations under this Agreement; and

2.1.3 If any actual or potential Conflict of Interest arises under this Agreement, the Supplier shall immediately and in all cases within three (3) days inform Etisalat Afghanistan in writing of such conflict and shall provide all relevant information to assist Etisalat Afghanistan in its assessment of such conflict.

3.1 The Supplier shall ensure that any third party associated with the Supplier who is performing services or providing goods in connection with the performance of this Agreement does so only on the basis of a written contract which imposes on such third-party terms equivalent to those imposed on the Supplier in this Annex 1. The Supplier shall be responsible for the observance and performance by such third parties of the terms similar to those stipulated by this compliance provisions and shall be directly liable to Etisalat Afghanistan for any breach by such third parties of any of the Relevant Requirements. For the purposes of this Annex 1, a person associated with the Supplier includes any subSupplier of the Supplier. The Supplier may only engage a third-party (e.g., subSupplier) under this Agreement subject to Etisalat Afghanistan's prior written approval.

3.2 In connection with its relationship to Etisalat Afghanistan and each of the transactions established by the Agreement, the Supplier has maintained and will continue to maintain complete and accurate books, records, invoices and other documents concerning payments and expenses.

3.3 Etisalat Afghanistan or its auditors or representatives may at any time audit Supplier's compliance with this Annex 1, and the Supplier warrants its full cooperation with any investigation of suspected violations, including but not limited to, the timely provision of all relevant information, records, documentation, evidence, and employees, as may be requested by Etisalat Afghanistan.

3.4 Etisalat Afghanistan shall be entitled to suspend payments of Supplier invoices that are, or become due in case there is a reasonable believe that the Supplier might have committed an actual or potential violation of this Annex 1 or applicable anti-bribery or anti-corruption laws, or whenever investigation or audit conducted reveal actual or suspected violations of this Annex 1, or that become due at any time during a period of ninety (90) days thereafter.

3.5 The Supplier shall indemnify Etisalat Afghanistan against any losses, liabilities, damages,

[1] *"Public Official," for the purposes of this agreement, includes, but is not limited to: (i) any elected or appointed official (whether in the executive, legislative or judicial branches of government) of a local, state, provincial, regional or national government (or any department or agency of those types of government bodies), (ii) any government employee, part-time government worker, unpaid government worker, or anyone "acting in an official capacity" (i.e., acting under a delegation of authority from a government to carry out government responsibilities), (iii) any political party, party official, or candidate for political office, (iv) any official or employee of a public international organization such as the World Bank or United Nations, or any department or agency of those types of organizations, (v) any official, representative, or employee of a company that is under even partial ownership or control by a government.*

costs (including but not limited to legal fees) and expenses incurred by, or awarded against, Etisalat Afghanistan as a result of any breach of this Annex 1 by the Supplier.

3.6 Breach of this Annex 1 shall constitute a material breach of this Agreement by the Supplier. If the Supplier is in breach of this Annex 1:

(a) Etisalat Afghanistan shall have the right to terminate this Agreement with immediate effect and suspend all payments, without prejudice to its rights and remedies under this Agreement, including its right to claim damages; and

(b) the Supplier shall not be entitled to any claim compensation or any further remuneration, regardless of any agreements entered into with third parties before termination.

2. Export Controls and Sanctions
Definition Section:

Affiliated Persons	mean any owner, officer, director, partner, principal, employee, any legal entity with control of or controlled by the Supplier or same owner(s) and/or or agents, suppliers or other Suppliers of the Supplier.
Applicable Sanctions/Export Control Laws	mean the Sanctions Laws and/or the Export Control Laws of the UAE, and any other jurisdiction in which the Supplier deals in Items and/or provides services [including but not limited to US, UK, EU].
Blocked Person	means, at any time, any person (a) whose property or interest in property is blocked by any Sanctions, (b) designated as a target of asset freeze under Sanctions, (c) with whom dealings are otherwise prohibited under applicable Sanctions or Export Control Laws, or (d) owned or controlled by any such person.
Export Control Laws	mean laws and regulations related to the regulation of imports, exports, re-exports, sale, resale, transfers, releases, shipments, transmissions, or any other provision or receipt of goods, technology, technical data, software, or services, and any laws or regulations of a similar nature administered and enforced by Governmental Authorities.
EU	Means the European Union
Governmental Authorities	mean any agency, office, bureau, department, or instrumentality of the national government of the UAE, [any other applicable jurisdiction: US, UK, EU], that is responsible for administering and enforcing Sanctions and Export Control Laws and/or which has other relevant regulatory or other authority over the Supplier, as required in the context of the relevant Agreement.
Item	means hardware, software including source code, technology, documents, technical data, diagrams and services.
Representatives	mean any third-party employed to act for or on behalf of Supplier including, without limitation, agents, Suppliers, sub-Suppliers and professional representatives.
Sanctions Laws	mean economic or financial sanctions or trade embargoes imposed, administered or enforced by Government Authorities with applicable jurisdiction.
Sectoral Sanctioned Entity	means, at any time, any person subject to Sanctions administered or enforced Governmental Authorities.

US	Means the United States of America
UK	Means the United Kingdom of Great Britain and Northern Ireland
UAE	Means the United Arab Emirates

Sanctions and Export Control clauses:

[1. The Supplier acknowledges that any Items that it provides under the Agreement may be subject, or become subject in the future, to the Applicable Sanctions/Export Control Laws of one or more jurisdictions (including without limit those of the U.S., the European Union, the UAE, the UK and any other jurisdiction in which it deals in Items), and shall not deal in, supply, deliver, broker or export any such Items without first obtaining all governmental licenses and approvals and making any notifications that may be required under such Applicable Sanctions/Export Control Laws.]

2. The Supplier agrees at all times to comply with and ensure that it, its Affiliated Persons and Representatives act in compliance with all Applicable Sanctions/Export Control Laws in carrying out its responsibilities under this Agreement. Without limiting the foregoing, the Supplier represents, warrants and undertakes that:

2.1 Neither the Supplier, nor any of its Affiliated Persons or Representatives is a Blocked Person, Sectoral Sanctioned Entity, or otherwise sanctioned person/entity with whom dealings are prohibited or restricted under the Applicable Sanctions/Export Control

Laws;

2.2 The Supplier will not, in connection with any activities involving [Etisalat Afghanistan] (including all Affiliated persons or representatives of [Etisalat Afghanistan]) or this Agreement, export, re-export, ship, sell, resell, supply, deliver, or otherwise transfer any Items to, from, or through – either directly or indirectly – any country or person in violation of any Applicable Sanctions/Export Control Laws;

2.3 The Supplier will not cause [Etisalat Afghanistan] to violate any Applicable Sanctions/Export Control Laws;

2.4 The Supplier shall provide to [Etisalat Afghanistan], prior to delivery of any Items that would be classified under applicable Export Controls, [i] a schedule identifying in writing the export controls regime to which the Items are subject and, [ii] the appropriate export controls classifications (e.g., Export Control Classification Numbers) with respect to each Item, in sufficient detail to enable [Etisalat Afghanistan] to ascertain any export control that may apply to [Etisalat Afghanistan]; and

2.5 The Supplier shall promptly notify [Etisalat Afghanistan] in writing of any suspected or confirmed violations or issues of non-compliance involving any Items provided to [Etisalat Afghanistan], and in any case no later than within 3 days.

2.6 The Supplier shall notify [Etisalat Afghanistan] in writing as soon as possible if:

(i) the Supplier, or any of its Affiliated Persons or Representatives, has become listed on any restricted parties list (including, without limitation, any US, EU, UK or UN sanctions lists) or becomes subject to any Sanctions; or

(ii) it becomes aware that any relevant Governmental Authority has initiated or will initiate any investigation or proceedings against the Supplier, or any of its Affiliated Persons or Representatives, relating to an actual or potential breach of any Export Control Laws or Sanctions in relation to its obligations under this Agreement.

3. The Supplier shall identify, obtain and maintain all government registrations, licenses and approvals required under any applicable Export Control Laws to engage in the activities covered by this Agreement, including any applicable registrations or licenses to engage in the business of manufacturing, exporting, brokering or trading export controlled Items.

4. Nothing in the Agreement is intended, and nothing herein should be interpreted or construed, to induce or require either Party or their Affiliated Persons or Representatives to act in any manner which is inconsistent with, penalized, or prohibited under any Applicable Sanctions/Export Control Laws as applicable to such Party;

5. Neither party nor its Affiliated Persons or Representatives shall be obliged to perform any obligation otherwise required under this Agreement if this would be in violation of, inconsistent with, or expose such party to punitive measures under, any Applicable Sanctions/Export Control Laws.

6. If [Etisalat Afghanistan], acting reasonably, believes that the Supplier, its Affiliated Persons or its Representatives breached or is likely to have breached any element of these Sanctions and Export Control clauses, [Etisalat Afghanistan] shall have the right to immediately conduct an appropriate audit into any such breach or potential breach, using its own resources and/or through independent third parties engaged by [Etisalat Afghanistan], and shall withhold payments to the Supplier during the period of any such audit. Supplier, its Affiliated Persons or its Representatives shall at all times cooperate fully and in good faith including with regard to the prompt provision of all relevant information, records and documents in order to facilitate and expedite the conduct of any such [Etisalat Afghanistan] audit.

7. The Supplier agrees that non-compliance with any of the representations and/or obligations set out in this Agreement by the Supplier, its Affiliated Persons or its Representatives may result in adverse consequences for [Etisalat Afghanistan] and would allow [Etisalat Afghanistan] to consider such non-compliance as a material breach of the Agreement, and would further entitle [Etisalat Afghanistan] to immediately terminate any and all existing Agreements with the Supplier for cause without liability as specified in the Agreement.

8. The Supplier agrees to fully indemnify and hold harmless [Etisalat Afghanistan] and its representatives against any damages, costs, losses, liabilities, fines, penalties, and/or expenses (including attorneys' fees and expenses) arising out of and in connection with the Supplier, its Affiliated Persons or Representatives non-compliance with these Sanctions and Export Control clauses, including violation or alleged violation of any Applicable Sanctions/Export Control Laws.

9. The Supplier agrees that [Etisalat Afghanistan] may, at its sole discretion, conduct surveys and audits (either directly or through independent third parties engaged by [Etisalat Afghanistan]) to verify compliance by the Supplier, its Affiliated Persons and Representatives with these Sanctions and Export Control clauses and Applicable Sanctions/Export Control Laws. Such surveys or audits shall be reasonable as to scope, location, date and time. The Supplier, its Affiliated Persons or Representatives) shall cooperate fully and in good faith with any such survey or audit including

the prompt provision of all relevant information, records and documents as [Etisalat Afghanistan] may reasonably require in order to facilitate and expedite the conduct of any such audit.

10. In the event that [Etisalat Afghanistan] is required to obtain an authorisation, licence or other governmental approval or to make a notification under Applicable Export Control Laws for reasons arising out of this Agreement or the acts contemplated by it, the Supplier shall provide such assistance to [Etisalat Afghanistan] in obtaining such approval as [Etisalat Afghanistan] may reasonably require.

3. Anti-Money Laundering and Counter Finance of Terrorism:

1. "**Applicable Anti-Money Laundering Laws and Counter Finance of Terrorism" or "AML/CFT**" means any laws, rules, or regulations applicable to [Etisalat Afghanistan] and the Supplier, that prohibit engaging in or facilitating financial transactions that promote or conceal unlawful activity in any jurisdiction.

2. The Supplier represents and warrants that:

i. the Supplier and each of its affiliated persons will refrain from engaging, whether directly or indirectly, in improper and/or illegal conduct, including money-laundering and terrorist financing; and, where applicable, will comply with Applicable AML/CFT Laws;

ii. If applicable, the Supplier has in place procedures aimed at preventing AML/CFT violations; and

iii. the Supplier agrees to notify [Etisalat Afghanistan] promptly and in any event within 3 days, in writing, of any suspicious activity under AML/CFT Laws, of which it becomes aware relating to the transaction involving Etisalat Afghanistan. Upon reasonable request, the Etisalat Afghanistan agrees to provide Etisalat Afghanistan with documentation relating to its AML/CFT policies and procedures and assist [Etisalat Afghanistan] with any clarification required without any undue delay.

Annexure-D

Cybersecurity Requirements

General Security Requirements:

1. Vendor must ensure their operating systems are up to date and is not End of Life/End of Support.
2. Vendor must ensure proper patch management of their servers in alignment with EA IT and Cybersecurity policies.
3. Vendor must ensure a licensed and standard AV solution is installed in all of their operating systems.
4. Vendor must ensure full cooperation and coordination with EA Cybersecurity team whenever required.
5. Vendor must not install any application without proper coordination and agreement of EA SOC Team.
6. The use of insecure cryptographic algorithms and protocols are strictly prohibited and all integrations and system communication must be based on secure and strong cryptographic algorithms.
7. Vendor must ensure strong protection of EA data stored on vendor's cloud.
8. Vendor must align all of their services and configurations in accordance to EA Information Security policies and standards.
9. Vendor must use and install only licensed applications.
10. The installation and Integration of servers must be aligned with IT and Cybersecurity requirements.
11. Vendor must not use/install any application/service that is not required.
12. Vendor must communicate any software installation with EA Cybersecurity team in advance.
13. Vendor must align their changes according to EA Change Management Policy.
14. Vendor must ensure all their operating systems are fully patched with the latest OS/Software updates.
15. Vendor must not use any OS that is/will be End of Life / End of Support in less than 3 year.
16. Only secure and strong cryptographic algorithms are allowed to be used in the vendor platforms.
17. System must support Role Based Access Control, and Rule Based Access Control
18. System must provide Strong authentication and authorization mechanisms
19. System must be capable of advanced logging mechanisms to ensure user activities are logged for audit and security purposes and the log must include all of the following at minimum.
    - Failed and successful logins
    - Modification of security settings
    - Privileged use or escalation of privileges
    - System events
    - Modification of system-level objects
    - Session activity
    - Account management activities including password changes, account creation, modification…
    - Event logs must contain the following details:
    - Date and time of activity
    - Source and Destination IP for the related activity
    - Identification of user performing activity
    - Description of an attempted or completed activity.
20. The system must support live log retention of 1 Year and backup up to 3 years.

21. System must be capable of encrypting the log files to ensure user does not modify or change the logs.
22. System must provide cryptographic algorithms such as AES 128/256 Bit, SHA 256/384/512 bits.
23. System must be secure against well-known attacks including but not limited to SQL Injection, XSS, CSRF, SSRF, Code Execution and other attacks.
24. Vendor system's password configuration must be aligned with EA Information security policies.
25. System must support integration with LDAP, IAM "Identity and Access Management" and PAM "Privileged Access Management" Solutions.
26. System must support external log synchronization mechanisms to push logs to another system for analysis such as SIEM and centralized log server.
27. The database must support the encryption of admin user's information with algorithms such as PBKDF2 and SHA256/384/512 bits.
28. The database platforms "if any" must support the encryption of data in-transit and at rest.

Important Note:

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

No.	Description	Compliance (YES/NO/NA)	Comments
1	**Etisalat Security Requirements**		
1.1	The Contractor/Supplier/vendor to sign Non-Disclosure Agreement (NDA) with Etisalat before finalizing RFx/contract/POC agreement as per Etisalat NDA process.		
1.2	Contractor/Supplier/vendor equipment's (e.g. Servers, PCs, etc.) that are connected to Etisalat network must be securely wiped before taking out of Etisalat premises.		
1.3	The proposed/contracted system shall pass Etisalat Security Audit (Vulnerability Assessment/Penetration Testing) before go-live/service acceptance by Etisalat. Contractor/Supplier/vendor shall provide SLA for fixing Security gaps based on severity.		
1.4	Contractor/Supplier/vendor shall fix all security issues identified and reported by ETISALAT and/or Third Party Contracted to do the testing, with no additional cost		
1.5	Contractor/Supplier/vendor confirms that its products/solution are tested for weaknesses via methods such as Vulnerability Assessment, penetration testing, red teaming exercises and scans that check for compliance against the baseline 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,		

No.	Description	Compliance (YES/NO/NA)	Comments
	PCI, ISO, GDPR etc.) The Contractor/Supplier/vendor shall confirm the applicable standard.		
2.2	The proposed solution shall support the latest operating systems and application versions. Contractor/Supplier/vendor to ensure proposed solutions will run the latest stable software, operating system, and firmware.		
2.3	The solution shall be designed with multi-tier architecture, (Demilitarized Zone (DMZ), middleware, and private network). Any system accessible from the Internet shall be on the DMZ and access to internal sensitive data shall be secured through the middle tier application proxy.		
2.4	The proposed solution shall not impact or relax existing Etisalat security control or posture.		
2.5	The performance of the proposed system shall meet the business requirements without disabling or removing any existing security control		
2.6	The Contractor/Supplier/vendor shall provide only secure methods of communication such as HTTPS, SFTP, SCP, TLS1.3, IPSEC, SRTP, SSH v2, SNMPv3 between the proposed nodes. Non-secure protocols such as Telnet, HTTP and FTP shall not be used.		
3	**Password Security**		
3.1	All Operating Systems (e.g. Linux and Windows) shall be hardened according to well-known standards such as, but not limited to NIST, CIS security benchmark, and NSA.		
3.2	The proposed system includes password management module that supports the following features:		
3.3	Setting the minimum password length		
3.4	Password complexity, and not accepting blank passwords		
3.5	Maximum password age and password history		
3.6	Account lockout		
3.7	Enforce changing password after first login		
3.8	Prompt / notify for the old password on password changes		
3.9	The password shall be saved in hashed format (i.e. irreversible encryption)		
3.10	Forgetting or resetting password function shall support using OTP or email for verification		
4	**Authentication**		
4.1	The proposed system shall not provide access without valid username and password.		
4.2	All user access to the proposed system shall support Privilege account Management (PAM) integration.		
4.3	For public web applications, the proposed system supports and uses CAPTCHA or OTP to prevent password dictionary attacks		

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, 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)		
5.2	The proposed system supports role-based access permissions, i.e. Administrator, Operator, Viewer, User…		
6	**Software Security**		
6.1	The software development and testing will not run on the production systems, and will be running in an isolated environment		
6.2	The software source code will not include clear-text passwords		
6.3	The software code will not include insecure protocols, like FTP, telnet ...etc.		
6.4	The software testing will not use live/production sensitive or PII data unless it's masked as Etisalat security policy		
6.5	The proposed system enforces input and output validation to prevent security attacks, like SQL Injection, Buffer Overflow…etc.		
6.6	For web portals, the proposed system includes all security controls to prevent/protect from OWASP Top 10 security attacks and risks		
6.7	For mobile application, the proposed system shall include security checks / controls to protect from mobile attacks, like SSL Pinning, Jailbreak, Anti-debug, Anti-hooking, and Advanced Obfuscation…		

No.	Description	Compliance (YES/NO/NA)	Comments
7	**Security Event Logging**		
7.1	Proposed systems shall support standard logging protocols such as CIFS/Syslog/CSV logs files		
7.2	The system shall generate and support audit logs that contain the following fields (as a minimum): a) Username b) Timestamp (Date & Time). c) Client IP Address d) Transaction ID & session information		
7.3	The proposed solution shall support the integration with Etisalat NTP for time synchronization and accurate logging.		
8	**Public Cloud Security**		
8.1	Etisalat customers' and staff personal data (PII: name, contacts, address, Emirates ID, Passport number, Nationality …) is encrypted at rest and in transit using a strong industry-standard encryption protocol		
8.2	The Public Cloud setup that stores PII information shall be hosted in the Afghanistan		
8.3	The Public Cloud setup is hosted in a dedicated tenant for Etisalat (i.e. not shared)		
8.4	The Public Cloud data Center shall not be moved to another country or location without prior coordination and approval from Etisalat		
8.5	All Etisalat data will be permanently erased from the Public Cloud on termination of the service or support agreement		
8.6	The proposed Cloud system supports Etisalat Cloud Access Security Broker (such as Microsoft MCAS, Netskope CASB)		
9	**Virtualization and Container Security**		
9.1	If applicable, Bidder shall ensure the proposed virtualized infrastructure, service based and micro services architecture to support multi tenancy, zoning & micro-segmentation, security visibility, secure virtualization (sVirt), trusted image signing, virtual Firewalls, DoS protection, Trusted platform module (TPM), Hypervisor & Host OS security to secure data and resources.		
9.2	The proposed solution shall support integration with Etisalat/Leading Container Security Solution, where applicable, to scan the container images and ensure malware protection of CI/CD pipeline.		
9.3	Suppliers must inform EA Cybersecurity of any non-		

	conformity with defined EA policies and processes that are agreed upon in advance to acquire a written approval from EA Cybersecurity Department or senior management as required otherwise Supplier will be responsible for all the potential losses		

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