TENDER NOTICE

No. EA/02-72-2026

Provision of e-Procurement Solution

1. Etisalat Afghanistan invites proposals from qualified and authorized providers or implementation partners for the provision, implementation, integration, data migration, training, and support of an e-Procurement Source-to-Pay software solution.

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. The deadline for submission of proposals is **23 November 2026**, **Afghanistan time**.

3. Proposals received after the specified submission deadline will 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.** Vendors must submit their proposals using the same email that is shared by EA. Any proposal submitted with a modified or incorrect subject/title of email may not be considered. EA shall not be responsible for proposals that are missed, delayed, or excluded due to non-compliance with this requirement.

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 complaints that meet all the mandatory

service-effecting requirements will be evaluated commercially.

6. EA 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 EA Afghanistan action.

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

Name: Ahmad Shikib Shalizi
Department: Procurement and Contracts
Email: Ashalizi@etisalat.af
Phone: +93786773777

Ihsanullah Zirak

Director Procurement and Supply Chain

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

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

(RFP)

For

Provision, implementation, integration, data migration, training, and support of an e-Procurement Source-to-Pay software solution 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 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 EA 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.

"EA 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 from authorized and qualified providers for the provision of e-Procurement platform, as specified in the RFP Annexures.

2.2 The tender award will be based on the best technical and unit rate, 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).
5.7 EA reserves the right to process Purchase Order (PO) or contract-related payments through the eMoney (mobile financial services) platform, directly to the Supplier's registered eMoney 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 Hardware & Software;

5.1.1 EA will make payment equal to 50% of the amount after delivery on the arrival and certification by EA Project Director/Manager of their receipt in good condition.

5.5.1.2 Balance 50% of the amount of hardware/software will be paid on issuance of RFS.

6.2 For Installation, Testing, Commissioning and Professional Services

6.2.1 EA will make payment equal to 75% of amount of Services cost after delivery of services an Acceptance Testing.

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.

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 EA 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. Annexures-D…….. Cybersecurity Compliance

Annexure-A (Scope of Work)

E-Procurement / Source-to-Pay – Scope of Work

Contents

1. Document purpose
2. Background
3. Business context and current-state challenges
4. Project objectives
5. Guiding principles
6. Overall scope
7. Target operating and capability model
8. Detailed work packages
9. D365 integration and system ownership
10. Workflow, governance and controls
11. Reporting and analytics
12. Security and non-functional requirements
13. Implementation scope
14. Data migration
15. Testing and acceptance approach
16. Training and documentation
17. Support, warranty and hypercare
18. In scope
19. Out of scope
20. Optional and future scope
21. Dependencies and assumptions
22. Stakeholder validation items
23. Acceptance criteria
24. Expected vendor / implementation deliverables

1. Document purpose

This SOW defines the consolidated business, functional, integration, governance and control scope for the E-Procurement / Source-to-Pay initiative. Procurement and Technical have reviewed and confirmed the scope applicable to their respective functions.

2. Background

Procurement and Technical scope confirmations have subsequently been received.

3. Business context and current-state challenges

Reported challenges include manual/email-based tendering, dispersed tender documents and approvals, risks of early bid access or alteration, weak end-to-end reporting/audit evidence and manual re-entry of award outcomes into D365. Procurement additionally identifies gaps in complete SRM and CLM coverage.

4. Project objectives

- Provide a controlled supplier lifecycle from registration and qualification through participation, contracts, acceptance, invoice collaboration and performance history.
- Preserve defensible sourcing-to-award decisions through secure bids, controlled evaluation, approvals and complete evidence.
- Manage contracts from preparation and review through execution, obligations, changes and closure.
- Connect supplier collaboration with D365 while retaining its financial and procurement transaction ownership.
- Give stakeholders authorised visibility of sourcing, commitments, contracts, acceptance, supplier performance and exceptions.

Expected value includes more consistent procurement administration, clearer evaluation/acceptance responsibilities, better financial traceability and one controlled supplier communication channel. Baselines and measurable improvement targets must be established during requirements validation.

5. Guiding principles

D365 authority. D365 owns the approved vendor master and downstream PR, PO, receipts, invoice posting, budget, tax/accounting, payments and GL. Supplier registration and qualification do not automatically create a vendor.

Evidence and ownership. Preserve source identifiers, approved versions and accountable decisions across systems. ATP means Acceptance Test Procedure / acceptance process in this SOW.

6. Overall scope

The baseline comprises WP1 Source-to-Award, WP2 SRM, WP3 CLM and WP4 Supplier Collaboration, with D365 integration and shared analytics, governance, security and delivery requirements. WP5 Source-to-Asset remains optional. Module packaging and rollout priority remain open. The platform

boundary covers upstream business records, collaboration, evidence and workflows; D365 retains transactional execution.

7. Target operating and capability model

Capability domain	Primary responsibility	Scope mapping
Source-to-Award / E-Sourcing	Sourcing events, confidential bids, evaluations and award	WP1
Supplier Relationship Management	Registration, qualification, due diligence, performance and history	WP2
Contract Lifecycle Management	Drafting, reviews, execution, obligations, amendments and closure	WP3
Supplier Collaboration	Supplier access, PO visibility, ATP and invoice collaboration	WP4
D365 integration	Controlled handoffs and authoritative financial/procurement transactions	Section 9; Deliverable 3
Analytics, governance, security and audit	Shared reporting, approvals, access, evidence and operational controls	Sections 10–12

Lifecycle relationships. Registered Supplier → Qualified/Approved Supplier describes platform eligibility states. A D365 Vendor is a separate financial-master identity created or reused only at the approved qualification/approval/award gate. Sourcing Event → Award → Contract → D365 Vendor → PR/PO describes linked records, not a mandatory chronology: a PR or vendor may already exist.

8. Detailed work packages

8.1 WP1 – Source-to-Award / E-Sourcing

SRC-01 Sourcing initiation. Capture a sourcing request with business need, category, requester, scope/specification, required dates and supporting documents. Link an existing D365 PR where applicable; a sourcing request is not a replacement PR or a budget reservation.

SRC-02 Sourcing routes. Support RFQ and RFP events, and RFI where applicable, with distinct templates and steps. Procurement shall validate the sourcing routes, approvals and any permitted exceptions before configuration.

SRC-03 Tender preparation. Prepare controlled tender packs containing the specification, submission instructions, technical/commercial response schedules, evaluation criteria and required documents. Maintain template versions and event approvals.

SRC-04 Bidder invitation and publication. Identify and invite eligible bidders, record invitations and responses, and publish tenders where the approved sourcing route requires it. Apply the validated qualification/participation rules without treating registration alone as approval.

SRC-05 Clarifications and communication. Provide an event-linked channel for bidder questions, authorised replies and notifications. Preserve sender, recipients, attachments and timestamps; apply the approved rules for common clarifications and confidential bidder-specific information.

SRC-06 Addenda and deadlines. Issue controlled tender addenda with version history and notification evidence. Record the authority, reason and time for any approved deadline or requirement change, and clearly identify the current tender pack.

SRC-07 Online bid submission. Allow bidders to submit technical and financial/commercial offers securely against the correct event. Record submission time, bidder identity and a receipt; enforce the published deadline and retain submission/replacement history under the approved tender rules.

SRC-08 Sealed-bid confidentiality. Prevent premature or unauthorised access to submitted bids, including financial offers before the authorised release stage. The design must address privileged/support access as well as ordinary evaluator access and provide evidence that confidentiality controls operate.

Demonstrate that vendor/support personnel, database administrators and backup operators cannot read submitted bids before authorised opening. Document encryption-key custody, controlled opening, trusted timestamps and approved handling of late submissions, deadline extensions and outages.

SRC-09 Controlled bid opening. Release offers only to authorised opening/evaluation roles at the approved time or stage. Preserve the opening record, participants, timestamps and accessed/released offer versions; the committee composition and technical/financial opening sequence require validation.

SRC-10 Technical evaluation. Assign technical evaluators and committee access to the relevant event and offers. Record structured criteria, scores, comments, supporting evidence and evaluation outcome through the validated technical review/approval workflow.

SRC-11 Commercial evaluation. Support controlled financial/commercial evaluation using the approved criteria and comparable bid information. Restrict financial offer access, record clarifications and evaluation evidence, and route the commercial outcome for the validated approvals.

SRC-12 Scoring integrity. Support structured scoring and weighted scoring where applicable. Preserve the criteria/weight version, evaluator input, calculation and approved outcome; later changes must be authorised, explained and retained rather than silently changing the evaluation record.

SRC-13 Negotiation and BAFO. Record negotiation rounds, participants, communications and revised offers. Support best and final offer (BAFO) where the approved route permits it, retaining earlier offers and the authority for requesting another round.

SRC-14 Award recommendation and approval. Compile the award recommendation with evaluation results, justification, selected supplier(s), scope/value where applicable and supporting evidence. Route it through the approved authority structure and retain approval comments and timestamps.

SRC-15 Award record and notifications. Maintain the final approved award record, notify suppliers through controlled communications and preserve the notification history. Any change to an approved award must follow a controlled review and approval path.

SRC-16 Source-to-award lineage. Preserve retrievable links from sourcing request and event to tender version, submissions, opening, evaluations, negotiation, award and contract handoff. Carry approved event/award references into the relevant D365 transaction links without forcing a single PR timing for every route.

8.2 WP2 – Supplier Relationship Management

SRM-01 Registration and supplier profile. Support supplier self-registration, profile/contact details, category/classification and supporting documents. Issue a platform supplier identifier and track onboarding progress; a registered supplier is neither automatically qualified nor a D365 vendor.

SRM-02 Qualification and approval. Provide qualification assessment, review, request-for-information, approval and rejection with reasons and evidence. Record qualification scope/status and the responsible approver separately from D365 vendor status.

SRM-03 Due diligence. Apply a configurable category-based due-diligence and required-document checklist. Capture review outcomes, responsible reviewers, outstanding items and evidence; Compliance and the relevant business owners must define documents, checks and exception rules.

SRM-04 Document validity and expiry. Record document type, upload/version, validity dates and expiry where applicable. Notify responsible users/suppliers of expiry and renewal needs while retaining prior records; the effect of expiry on qualification or transactions requires validation.

SRM-05 Supplier lifecycle status. Maintain approved, rejected, suspended/blocked and reinstated lifecycle outcomes where applicable, with effective dates, reasons and approval history. Participation restrictions shall follow agreed policy and shall not silently alter D365 financial processing.

SRM-06 D365 vendor distinction. Keep platform supplier and D365 vendor identifiers separately linked. A vendor creation/reuse request may proceed only after the applicable qualification/approval/award gate; Finance must validate the precise trigger and master-data authorisation.

SRM-07 Controlled profile changes. Retain the history of supplier/contact/document changes and route changes requiring approval to authorised internal reviewers. A supplier update in the portal must not directly overwrite approved D365 master data.

Sensitive changes, particularly bank details and authorised contacts, shall require independent verification and maker-checker approval. Retain verification and approval evidence; such changes shall not automatically overwrite approved D365 master data.

SRM-08 Performance review framework. Define supplier performance criteria, scoring, review frequency and responsible evaluators. Capture periodic reviews, comments, evidence and approved outcomes; ownership and review rules remain subject to business validation.

SRM-09 Performance history and indicators. Retain historical review scores, observations and follow-up actions, including supplier risk/compliance indicators where applicable. Do not make a score automatically suspend a supplier unless that business rule is separately approved.

SRM-10 Central supplier history. Provide a permission-controlled supplier record linked to sourcing participation, awards, contracts, ATP/acceptance and appropriate invoice interactions. Financial facts shall reference D365 records/statuses and indicate their source and freshness.

8.3 WP3 – Contract Lifecycle Management

CLM-01 Contract initiation. Create a contract request linked to the approved award or another validated contracting route. Capture the supplier, category, scope, proposed owner and supporting commercial/technical material needed to begin drafting.

CLM-02 Templates and clauses. Prepare contracts from standardised templates with an identified template owner, version and approval history. Support clauses where applicable; authority to approve or change standard wording requires Procurement/Legal validation.

CLM-03 Draft preparation and versions. Maintain successive contract drafts and their authors, dates and supporting documents. Preserve version comparisons or redlining/change history where supported so reviewers can identify changes to commercial terms, scope and obligations.

CLM-04 Cross-functional review. Route drafts for Procurement and applicable Legal, Technical, Finance/commercial and management review. Record each review outcome, comments, attachments and returned revisions; required routes vary only under validated business rules.

CLM-05 Approval authority and delegation. Configure contract approval workflows to the validated delegation of authority (DOA), including permitted temporary delegation. Retain who acted, on whose authority, for which version, when and with what comments.

CLM-06 Controlled supplier circulation. Communicate and circulate contract drafts to the intended supplier/contractor through a controlled channel. Record the version shared, recipients, response, comments and returned document without losing prior versions.

CLM-07 Approval of final version. Clearly distinguish draft, under-review, approved-for-execution and executed records. Changes after approval must be visible and routed for the required reapproval; the executed record must be linked to the approved version or an authorised, explained variation.

CLM-08 Execution and signing evidence. Support the validated signing/execution process and retain the final executed document, signatory evidence and execution date. Electronic signing services or assumed legal equivalence are not prescribed; acceptable signing methods require Legal/Compliance validation.

CLM-09 Contract repository. Maintain a central, searchable contract repository containing executed contracts and supporting documents, with role-based access and complete amendment history. Restrict access to confidential contract content to authorised roles.

CLM-10 Contract metadata and ownership. Record contract ID, supplier and applicable D365 vendor link, contract owner, effective/start and expiry/end dates, value/currency where applicable, status and related award. Maintain accountable owners and approved metadata changes.

CLM-11 Obligations and delivery milestones. Record contractual milestones, deliverables and obligations with due dates, evidence and responsible owners. Provide reminders and escalation/visibility for overdue items according to the validated process.

CLM-12 Expiry, renewal and extension. Provide expiry and key-event alerts with enough configurable notice to support business review. Route renewal and extension requests for required reviews/approvals and retain the resulting term and version history.

CLM-13 Amendments and changes. Control requests to change scope, value, dates, obligations or contract documents. Record the reason, prior and revised versions, impact and approvals, and identify affected D365 references for authorised downstream action.

CLM-14 Closure and retained history. Record contract closure, outstanding obligations/disputes where applicable, approval and supporting evidence. Retain executed documents, reviews, amendments and activity history under the approved retention rules.

CLM-15 Contract-to-D365 relationship. Preserve sourcing event → award → contract → D365 vendor → PR/PO references as linked records. This expresses traceability: a PR may precede sourcing and a vendor may already exist.

8.4 WP4 – Supplier Collaboration

COL-01 Supplier portal access. Provide authenticated supplier access to permitted records for that supplier and its authorised contacts. Apply external-user security, account lifecycle controls and confidentiality boundaries; internal information shall not become visible merely because D365 is integrated.

Apply malware scanning, permitted file-type and size restrictions, safe document handling, secure session controls and protection against automated abuse. The vendor shall describe its proposed web application and denial-of-service protection.

COL-02 Supplier collaboration channel. Allow permitted profile access and controlled communication across qualification, sourcing, contracts, ATP and invoices. Retain messages, attachments and notification history against the relevant record with appropriate access restrictions.

COL-03 PO visibility. Provide supplier-specific visibility of approved PO information received from D365. Finance/Procurement must validate fields and release stages; PO accounting, approval and changes remain controlled in D365.

COL-04 PO acknowledgement. *Proposed for stakeholder validation.* If business-approved, capture supplier acknowledgement and queries against the D365 PO version shared. An acknowledgement shall not change a D365 PO or imply receipt/acceptance; inclusion requires validation.

ATP-01 ATP record and evidence. Digitise the Acceptance Test Procedure / acceptance process for applicable goods/services. Capture the submitting party, related supplier/contract/PO references, acceptance details, dates and supporting evidence required by the validated process.

ATP-02 Acceptance review. Route ATPs to authorised reviewers with the relevant evidence and record findings, comments, clarification requests and revisions. Support the validated responsibilities for supplier submission and internal technical/business review.

ATP-03 ATP approval or rejection. Record approval/rejection, accountable reviewers/approvers, timestamps and supporting comments. Where partial acceptance applies, the accepted scope must be identifiable under the rules validated by Technical, Procurement and Finance.

ATP-04 Protection of approved ATPs. Prevent free editing or replacement of an approved ATP and its approved evidence. Preserve the exact approved version and evidence with submitter, reviewers, approvers, date/time and approval history; include privileged activities in the audit trail.

ATP-05 Controlled supersession and reapproval. Handle approved ATP amendments, corrections or replacements through a linked superseding version with a reason for change and required reapproval. Retain all prior versions/evidence and identify the current effective approved record; do not silently rewrite historical approval.

ATP-06 Acceptance as an invoice control. *Proposed for stakeholder validation.* Make the applicable ATP status/version and evidence available for downstream control. Finance, Procurement and Technical will decide where this affects invoice processing, how it relates to GRN/service confirmation and what happens after supersession.

INV-01 Supplier invoice submission. Allow suppliers to submit invoice details and supporting documents against the appropriate vendor/PO/contract and acceptance references where applicable. Capture a portal submission ID, submitter and time; submission alone is not D365 accounting acceptance, posting or payment approval.

INV-02 Document and clarification handling. Apply the validated supporting-document requirements and allow authorised users to request clarification or reject a submission with reasons. Retain the original submission, responses and corrected versions.

INV-03 Controlled D365 invoice handoff. Transfer validated invoice information and evidence through the approved interface for D365 processing. Maintain portal and D365 document identifiers separately and return an integration acknowledgement or actionable exception; do not post from the portal.

INV-04 Invoice accounting boundaries. Retain D365 ownership of invoice validation/accounting, posting, tax treatment, financial approvals and payment. Portal collaboration shall not bypass applicable D365 controls or create an alternative financial ledger.

INV-05 Invoice progress and rejection visibility. Show only approved supplier-facing status, rejection/clarification reasons and required actions. Distinguish portal submission/review from D365 receipt/processing/posting status, identify the source and refresh time, and avoid presenting a failed transfer as successful ERP processing.

INV-06 Payment-status visibility. *Proposed for stakeholder validation.* Provide payment/status information only where Finance and IT approve the business need, fields and technical availability. Use D365 as the source; exclude sensitive internal/banking information unless specifically authorised for disclosure.

8.5 WP5 – Source-to-Asset (optional)

AST-01 Optional asset lineage. Optional / subject to stakeholder validation: link approved sourcing, award, contract, PO, receipt and ATP evidence to relevant D365 asset or project references for asset-acquisition traceability. Validate the actual handoff points before including WP5 in the baseline.

AST-02 Optional asset handoff controls. Optional / subject to stakeholder validation: define required asset-identification, custody/handover and evidence links only for the agreed acquisition scenarios. Asset creation, capitalisation, depreciation and asset accounting remain in D365; a new asset-management platform is not included.

9. D365 integration and system ownership

INT-01 Transactional system of record. D365 Finance & Operations remains authoritative for approved vendor master, PRs, POs, GRN/receipts, invoice accounting/posting, budget control, payment, tax/accounting and general ledger. The platform owns upstream/collaboration records as described in the separate ownership matrix.

INT-02 Vendor creation and changes. Allow D365 vendor creation or reuse only through the approved post-qualification/approval/award process and authorised master-data controls. Return the D365 vendor ID to the platform, reconcile links and prevent registration or qualification alone from creating a financial vendor.

INT-03 PR, sourcing and award references. Keep PR ownership and budget checking in D365. Exchange only the approved request/status/reference data needed for sourcing, and preserve event/award references for downstream traceability; initiation timing and the permitted handoff route require validation.

INT-04 Contract and PO linkage. Retain executed contract and lifecycle records in the platform while linking relevant contract/award identifiers to D365 vendor/PR/PO records. D365 remains authoritative for the PO; an amended contract must not silently overwrite its financial commitments.

INT-05 ATP, receipt and invoice links. Preserve distinct ATP, D365 GRN/service-confirmation and invoice references. ATP approval is not automatically a D365 receipt or invoice posting; required status exchanges and any invoice gating are subject to Finance/Procurement/Technical validation.

INT-06 Financial status and visibility. Source approved invoice/payment status and internal commitment/spend facts from D365. Apply audience-specific field restrictions and show synchronization freshness; the platform must not calculate a competing authoritative payment or GL balance.

INT-07 Ownership and interface specification. Produce an approved interface catalogue covering object ownership, field authority, direction, trigger, identifiers, transformations, acknowledgements, frequency, security and exception ownership. Separate read-only projections from authorised transactional requests.

The interface catalogue shall include the API inventory and security requirements specified under SEC-04.

INT-08 Secure on-premises connectivity. Require a secure, supportable integration architecture for the actual on-premises D365 environment. Do not assume direct inbound Internet connectivity; the implementation provider must propose the connectivity pattern and demonstrate compliance with IT-approved controls.

The approved connectivity design shall enforce the applicable API and service-identity controls under SEC-04.

INT-09 Reliable integration operations. Require correlation IDs, duplicate-safe processing, controlled retry/replay, reconciliation and monitored exception queues so connection failures do not create duplicate vendors/invoices or lose approved evidence. Assign operational owners and acceptance evidence. Document reconciliation frequency, exception ownership, escalation timelines and closure evidence; define detailed implementation arrangements during solution design.

10. Workflow, governance and controls

GOV-01 Configurable approval workflows. Configure workflows, approval authority and permitted delegation against validated roles and DOA. Record acting user and delegated authority, and preserve pending/completed decisions when roles or workflow versions change.

GOV-02 Segregation and maker-checker. Apply role-based access and maker-checker/segregation rules to the relevant supplier, sourcing, evaluation, contract, acceptance and financial handoff activities. Compliance and business owners must validate incompatible roles and the handling of conflicts of interest.

Define and test incompatible roles, including supplier creation versus approval, bid administration versus evaluation, and invoice submission versus approval. Administrative access shall not permit unrecorded bypass of approvals or alteration of approved records.

GOV-03 Approval evidence. Retain workflow version, submitted record/version, decision, reviewer/approver, date/time, comments and supporting evidence. Users must be able to retrieve the complete approval history for an individual supplier, tender, contract, ATP or invoice interaction.

GOV-04 Controlled records and amendments. Preserve time-stamped, tamper-evident records, evidence and prior versions. Changes to approved records must follow the applicable amendment/reapproval process and retain reasons; retention and disposal must follow validated rules.

GOV-05 Exceptions. Capture the reason, responsible authority, decision, supporting evidence and follow-up for approved process exceptions. Do not assume an override or emergency-access policy; business/Compliance approval is required before an exception route is enabled.

GOV-06 User and administrator activity. Log relevant supplier, internal-user and administrator actions, including access to confidential records, workflow/configuration changes and privileged actions. Protect logs from unauthorised alteration and make them available to authorised reviewers.

GOV-07 Review and project governance. Record nominated focal points, scope decisions, approved changes and accountable signatories.

11. Reporting and analytics

RPT-01 Sourcing operations. Report sourcing pipeline, tender/event status, stage dates, cycle time and bidder/competition counts from platform event records. Preserve definitions for included events, elapsed time and participation so figures can be reconciled to underlying records.

RPT-02 Supplier lifecycle and performance. Report registrations, qualification/status, outstanding/expiring documents and historical performance scores from platform records. Display evaluation period/criteria and any approved D365-derived delivery or financial indicators separately.

RPT-03 Contract management. Report contract status, owner, start/expiry dates, values where applicable, upcoming renewals and overdue obligations/milestones. Drill down to the relevant executed contract, amendment or obligation evidence.

RPT-04 Acceptance and invoice collaboration. Report ATP review/approval/rejection/supersession and portal invoice submission/clarification/rejection status. Show D365 processing/payment states only from authorised integrations and distinguish them from platform workflow states.

RPT-05 Spend, commitments and budget visibility. Provide approved internal spend/procurement views where data is available. Use D365 for financial commitments, posted invoice/payment and budget facts; agree measure definitions, currencies, periods, access and refresh rules before building combined reports.

RPT-06 Controls and audit. Report workflow ageing, exceptions, compliance issues, access/activity and audit history with authorised drill-down/export. Join source identifiers across systems without copying sensitive data into unrestricted reports.

12. Security and non-functional requirements

These requirements specify outcomes for design and validation, not a chosen hosting/security product or numerical service commitment. IT/Security and Compliance must confirm the architecture constraints, service targets and records policies.

The solution and delivery services shall comply with applicable approved EA Afghanistan cybersecurity policies covering access management, data classification, API security, patching, incident management, third-party risk, cloud security and exceptions. Confirm applicable policy versions during requirements validation and provide the relevant requirements to bidders. Require a control-by-control vendor compliance response, supporting evidence and declared deviations.

SEC-01 Identity and access lifecycle. Implement role-based access, segregation and controlled account provisioning/removal. Require corporate SSO for internal users and administrators, and MFA for internal users, administrators, remote vendor support and supplier accounts. Any exception requires approval under the applicable cybersecurity policy. Define account recovery, inactive-account suspension and periodic access reviews. Use named administrator accounts, integrate with the approved privileged access management solution where applicable, and permit vendor access only with approval for a defined period. Log privileged sessions and review emergency access. Prohibit routine shared or default administrative credentials.

SEC-02 Data and document protection. Encrypt information in transit and at rest and enforce access to supplier documents, confidential bids, contracts and evidence. Validate data classification, authorised sharing, hosting/location and external-user controls with IT/Security and Compliance.

Classify bids, contracts, supplier identity documents, banking information and telecom technical specifications using approved Public, Confidential or Restricted classifications, as confirmed by the relevant data owners. Control downloads, exports and email sharing, and provide compatibility with the Microsoft Purview implementation where technically supported.

Restrict network diagrams, infrastructure locations, configurations and security designs through event-specific access, approved sharing and traceable downloads.

Disclose hosting, backup, disaster-recovery and support-access locations and relevant subcontractors. Contractual obligations shall address confidentiality, approved data use and audit rights. Enterprise data shall not be used for AI training without explicit authorisation.

SEC-03 Audit integrity. Protect time-stamped workflow and activity logs, approved evidence and document versions against unauthorised modification. Demonstrate how alterations or privileged actions are detectable and how records remain retrievable during the approved retention period.

SEC-04 Interfaces and environments. Provide supportable API/integration capabilities, controlled service identities and secure connectivity approved for D365. Document the environment and access model for development, testing and production; specific products or network topology are not prescribed.

Maintain an API inventory and apply scoped service identities, credential rotation, server-side authorisation, input validation, rate limits and controlled versioning. Test that changing supplier, invoice or document identifiers cannot expose another supplier’s records, using the OWASP API Security Top 10 as a testing reference.

Prohibit unauthorised publication of credentials, tokens, confidential API specifications, internal endpoints, configurations and enterprise data on public repositories or websites, including GitHub. Intentionally public API documentation requires approval before publication.

SEC-05 Availability and recovery. Define availability, backup, restore, disaster-recovery and business-continuity arrangements for service, documents, evidence and integrations. Validate recovery time (RTO), acceptable data loss (RPO) and restoration responsibilities; no numeric SLA is approved in this SOW.

Agree measurable availability, RTO, RPO, backup protection and restoration-testing requirements before contracting. Also agree concurrent bid-submission capacity and tender-deadline performance targets under SEC-06. Define how procurement activities will continue during an outage.

SEC-06 Performance and scalability. Size and test the solution for validated internal/external users, suppliers, events, concurrent bid submissions, document sizes, transaction volumes and growth. Agree measurable response/processing targets and critical tender-deadline workload before performance acceptance.

SEC-07 Monitoring and incident handling. Monitor service availability, failed integrations, background processing and security-relevant events. Define alert ownership, incident escalation, service reporting and recovery actions in the agreed operating/support model.

Integrate required security events with the approved SIEM and define alert ownership, incident notification timelines, evidence preservation, investigation support and root-cause reporting. Do not log passwords, tokens or sealed-bid contents. Include these obligations in the support contract and operating model.

SEC-08 Ownership, portability and maintainability. Preserve EA Afghanistan ownership of its business data and require usable export of records, documents, metadata and audit history. Document dependencies, licensing, custom components, upgrade/regression needs and handover arrangements to assess lock-in and long-term supportability.

SEC-09 Retention and disposal. Define and approve retention requirements by record type, including documents, logs, integration evidence and migrated records. Apply legal holds, controlled archiving and secure deletion, preserving retrieval and preventing conflicting retention or deletion across systems. Assign accountable owners and retain acceptance evidence for retention, disposal and vendor exit/export testing, including the usability and completeness of exported records, documents and audit history.

13. Implementation scope

IMP-01 Requirements and process validation. Run cross-functional workshops, confirm scope and process variants, maintain traceability by requirement ID and obtain the required baseline decisions. Capture roles, controls, exceptions, dependencies and prioritisation before detailed configuration.

IMP-02 Solution and delivery design. Produce a vendor-neutral fit/gap and solution design covering work packages, workflows, ownership, integrations, security, reporting and delivery options. Assess functional/control fit, D365 compatibility, five-year TCO, timeline, internal-resource dependency, sustainability and support without preselecting a product.

IMP-03 Configuration and approved customization. Configure agreed modules, forms, roles, templates, workflows, notifications and reports. Document any proposed customization, obtain approval for its need/cost/support impact, and maintain versioned configuration and technical documentation.

IMP-04 Integrated delivery. Build and document the approved interfaces/APIs, mappings and monitoring arrangements. Complete migration, workflow and cross-system integration work together with the D365 team and relevant business owners.

IMP-05 Cutover and production readiness. Prepare cutover, reconciliation, access readiness, support and rollback/contingency arrangements. Obtain agreed readiness evidence and authorisation before production use, including the treatment of in-flight sourcing, contracts, ATPs and invoice submissions.

IMP-06 Delivery plan and rollout. Provide a dependency-based plan for configuration, integration, tests, training and rollout. The indicative implementation period is 4–6 months after award; validate achievable dates, available resources and phasing after scope/architecture decisions rather than treating the estimate as a committed deadline.

14. Data migration

MIG-01 Migration inventory and scope. Inventory existing supplier data, D365 vendor links, active/historical contracts and supporting documents. Validate which records, history and cut-off dates migrate and which remain in a controlled legacy archive.

MIG-02 Preparation and reconciliation. Prepare mappings, clean data, identify duplicates, assign accountable owners and reconcile platform supplier IDs with approved D365 vendor IDs. Do not migrate a supplier record as a newly approved financial vendor or silently grant qualification status.

MIG-03 Trial loads and acceptance. Perform trial migration and controlled final loading with exception logs, count/key-field reconciliation, document-link checks and business sign-off. Preserve available provenance; gaps in legacy approval/evidence must be identified rather than invented.

15. Testing and acceptance approach

The test strategy must connect requirement IDs to business scenarios, roles, controls, data and expected outcomes. Section 23 supplies acceptance scenarios; scenario details must follow the stakeholder-approved process and architecture.

TST-01 SIT and traceability. Prepare system integration testing (SIT) scenarios mapped to requirements and data ownership, including successful paths, rejected requests, denied access and integration exceptions. Retain expected/actual outcomes, evidence and defect resolution.

TST-02 Cross-functional UAT. Execute user acceptance testing (UAT) with Procurement, Technical/IT, Finance, HR and Compliance against representative goods/services and approved process variants. Record business acceptance of workflows, roles, evidence and reporting.

TST-03 Security and confidentiality testing. Test supplier isolation, evaluator/administrator access, sealed-bid timing, segregation, document protection and audit history. Validate the implemented identity and secure D365 connectivity design through the IT-approved security assessment.

Require portal and API penetration testing, remediation and retesting. Retain evidence of access-control tests and sealed-bid demonstrations, together with recovery-test evidence under TST-04.

TST-04 Performance and recovery testing. Perform performance tests against agreed workloads/targets where required and verify backup/restore, continuity and integration recovery. Report results against the business-approved service criteria and address material gaps before acceptance.

TST-05 Defects and release acceptance. Maintain test evidence, defect priorities, remediation and retest results, and authorized acceptance records. Unresolved findings compromising bid confidentiality, supplier isolation, approved-record integrity or financial controls shall block release. Any permitted residual-risk exception requires documented justification, compensating controls, an expiry date and approval by the appropriate authorities.

Following product selection, agree the detailed severity-based release criteria, permitted exception route and remediation timelines with Cybersecurity and relevant business authorities before production release.

16. Training and documentation

TRN-01 Role-based training and change support. Train requesters, Procurement, evaluators, contract owners, Technical acceptance users, Finance, HR-related users, Compliance and support administrators as applicable. Provide supplier onboarding guidance and agree communications, champions and training responsibilities.

TRN-02 Business documentation. Deliver practical user guides, process/workflow maps, role guidance, tender/contract/ATP/invoice instructions and controlled templates. Include exception and amendment procedures so business users can operate and review the service.

TRN-03 Technical documentation and knowledge transfer. Deliver administration, security, configuration, integration/API, migration, monitoring, deployment and support documentation. Transfer knowledge to the designated IT/ERP and business support owners with retrievable configuration/source artefacts as applicable.

17. Support, warranty and hypercare

SUP-01 Hypercare. Provide a defined post-go-live hypercare period with named support contacts, issue tracking, prioritisation and operational monitoring. Agree duration, coverage and exit criteria with IT and business owners before contracting.

SUP-02 Warranty. Define warranty coverage, start/end conditions, defect correction, retesting and escalation responsibilities. Distinguish correction of delivered scope from separately approved change requests; no warranty duration or commercial entitlement is set by this SOW.

SUP-03 Ongoing support and upgrades. Define post-hypercare service ownership, support tiers, response/resolution targets, maintenance, upgrades, continuity and reporting. Record product/provider and internal responsibilities, annual recurring costs and knowledge-transfer obligations.

Require evidence of secure development, dependency scanning, security testing and supported component versions. Define patch responsibilities, policy-aligned vulnerability remediation commitments, end-of-support notification and approval of deviations. Use NIST SP 800-218 Secure Software Development Framework as an acquisition reference.

18. In scope

Include the baseline WP1–WP4 capabilities; required D365 handoffs; shared workflow, reporting, security and audit controls; requirements/process/solution design; configuration and approved customization; agreed migration; testing; training; documentation; deployment; and agreed hypercare, warranty and support. Conditional requirements become delivery commitments only when explicitly accepted through review.

19. Out of scope

The following boundaries apply to this SOW. Any proposed extension requires an explicit scope decision and impact assessment.

- Replacement of D365, a parallel financial ledger, external invoice accounting/posting, independent budget control or external payment execution.
- Automatic D365 vendor creation on supplier registration or qualification alone; unrestricted supplier access to internal D365 records.
- Unrelated D365 process redesign, an ERP/cloud migration, payroll processing or replacement of HR, warehouse or asset-management systems.
- A mandatory Source-to-Asset implementation, unapproved third-party services or a prescribed electronic-signature product/legal model.

20. Optional and future scope

WP5 remains optional and requires Finance-led validation with Technical, Procurement and IT. PO acknowledgement, supplier payment-status visibility and the precise ATP/invoice control rule remain conditional within WP4. Third-party signing, additional integrations, broader legacy-history migration or later rollout categories may be assessed only where a validated requirement justifies them; none is silently included.

21. Dependencies and assumptions

- Nominated focal points and timely decisions on supplier qualification, evaluation authority, CLM/Legal involvement, ATP and invoice controls.
- Current policies/DOA, due-diligence checklists, contract templates, retention requirements and approved process variants made available by their owners.
- IT confirmation of the actual on-premises D365 version/customizations, supported integration facilities, identity/hosting constraints, environments and technical resources.
- Agreed supplier/contract data quality, migration ownership, transaction volumes, service targets and supplier/user participation in testing and training.

22. Stakeholder validation items

Outstanding business, technical and cybersecurity decisions shall be confirmed by the relevant functions and recorded with the agreed outcome, approving authority, date and supporting evidence. The accompanying System Ownership and D365 Integration Matrix identifies proposed responsibilities and matters requiring confirmation.

23. Acceptance criteria

The following are draft acceptance criteria for validation.

AC-01 Supplier lifecycle. Register and qualify a supplier without creating a D365 vendor; demonstrate approved vendor creation/reuse only at the validated gate and retain mapped IDs.

AC-02 Bid confidentiality. Submit separate technical/financial offers; prove denied access before the authorised opening stage, deadline enforcement, permitted opening and complete event/access evidence.

AC-03 Evaluation and award. Complete the agreed technical/commercial scoring and approvals, including applicable negotiation/BAFO; retrieve the criteria version, comments, decision and supplier notification.

AC-04 Contract lifecycle. Create a template-based draft, complete applicable reviews, circulation and approval, capture execution, track obligations, and process an amendment/renewal/closure with full version history.

AC-05 ATP record integrity. Approve an ATP with evidence; demonstrate that the approved record cannot be freely edited and that a correction produces linked supersession/reapproval while preserving the earlier approved evidence.

AC-06 ATP/receipt/invoice rule. After Finance, Procurement and Technical approve the ATP/receipt/invoice rule, demonstrate the approved control for applicable accepted/partial/rejected/superseded cases and authorized exceptions, including the agreed treatment of invoices already processed.

AC-07 Invoice and payment ownership. Submit, clarify/correct and hand off an invoice; reconcile its portal/D365 identifiers and permitted statuses. Demonstrate that posting, tax, budget control and payment remain governed in D365.

AC-08 Supplier information boundaries. Verify supplier A cannot see supplier B data, confidential bids or unauthorised internal PO/invoice/payment information; validate evaluator and administrator access against approved roles.

AC-09 Integration and reconciliation. Reconcile vendor/award/contract/PR/PO/ATP/receipt/invoice links and demonstrate recovery from failed delivery. Prove duplicate-safe retry/replay, reconciliation and monitored exception resolution under INT-09.

AC-10 Cybersecurity assurance. Provide accepted portal/API penetration-test and retest results, access-control and segregation tests, sealed-bid demonstrations, and retention/disposal and exit/export evidence. Confirm that release-blocking findings are resolved and any permitted residual risks have time-bound approval under TST-05.

AC-11 Operational readiness. Provide accepted SIT/UAT/security and applicable performance/recovery results, agreed defect disposition, trained users, cutover evidence and complete business/technical/support documentation.

24. Expected vendor / implementation deliverables

The eventual provider or internal implementation team is expected to deliver the following outputs for

the approved scope. Review/acceptance authorities and contractual milestones will be finalised after stakeholder validation; this list does not establish a commercial commitment.

D01 Validated requirements and process baseline. Reviewed SOW, requirement traceability, process variants, agreed owners, roles/DOA and decision register.

D02 Solution and security design. Fit/gap, hosting/identity/security design, environment model, customization decisions and supportability assessment.

D03 System ownership and integration design. Approved matrix, interface catalogue, field mapping, identifiers, triggers, access rules, reconciliation and operating procedures.

D04 Configured solution. Working agreed modules, supplier portal, templates, workflows, controls, reports and authorised custom components.

D05 Training and documentation. User/supplier guidance, administrator and technical/integration documentation, training materials and knowledge-transfer evidence.

D06 Support and warranty package. Named support ownership, agreed hypercare/warranty/support terms, monitoring/escalation runbooks and service handover.

D07 Data and solution handover. Exportable data/documents/audit history, configuration and applicable source artefacts, dependency/license inventory and exit/portability procedures

Contract – Annexure B:

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

Content

1. SUPPLIER DEFINITION AND SCOPE 31
2. PURPOSE OF THIS CODE 31
3. SUPPLIER SELECTION AND ON-BOARDING 31
4. SUPPLIER MONITORING 32
5. DATA PROTECTION, PRIVACY AND CONFIDENTIALITY 32
6. MODERN SLAVERY, CHILD LABOUR, AND HUMAN TRAFFICKING 32
7. DISCRIMINATION 34
8. BRIBERY AND CORRUPTION 34
9. MONEY LAUNDERING 34
10. HEALTH & SAFETY 35
11. ENVIRONMENT AND CLIMATE CHANGE 36
12. SPEAK UP 36

1. Supplier Definition and Scope

1.1. The term **Supplier** means any person, entity or organization that provides or seeks to provide Etisalat Afghanistan with products, goods, or services. This includes all officers, employees, Suppliers, sub Suppliers, 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 recognize 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, labor standards, environmental, the responsible sourcing of minerals and health and safety.

2.5. The Supplier is encouraged to ensure its own Suppliers and sub Suppliers 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 authorized communication of Etisalat Afghanistan confidential or customer information should be limited to appropriately trained and authorized 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 Labor, 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 behavior.

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, organizations 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 organization, 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, (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

[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.*

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, 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
EA Cybersecurity Requirements

Overview

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

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

Important Note

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

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

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

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

No.	Description	Compliance (YES/NO/NA)	Comments
	to ensure proposed solutions will run the latest stable software, operating system, and firmware that is not End of Life or End of Support.		
2.3	The solution shall be designed with multi-tier architecture, (Demilitarized Zone (DMZ), middleware, and private network). Any system accessible from the Internet shall be on the DMZ and access to internal sensitive data shall be secured through the middle tier application proxy and/or a standard Firewall Technology.		
2.4	The proposed solution shall not impact the existing Etisalat Afghanistan security controls or posture in any way.		
2.5	The performance of the proposed system shall meet the business requirements without disabling or removing any existing security control.		
2.6	The Contractor/Supplier/vendor shall provide only secure methods of communication such as HTTPS, SFTP, SCP, TLS1.3, IPSEC, SRTP, SSH v2, SNMPv3 between the proposed nodes. Non-secure protocols such as Telnet, HTTP and FTP are strictly prohibited.		
3	**Password Security**		
3.1	All Operating Systems (e.g. Linux and Windows) must be hardened according to the official secure configuration baseline of Etisalat Afghanistan and to fully comply with Etisalat Afghanistan Security Policies.		
3.2	The proposed system includes password management module that supports the following features:		
3.3	Setting the minimum password length		
3.4	Password complexity, and not accepting blank passwords		
3.5	Maximum password age and password history/Threshold		
3.6	Account lockout		
3.7	Enforce changing password after first login		
3.8	Prompt / notify for the old password on password changes		
3.9	The password shall be saved in hashed format (i.e., irreversible encryption)		
3.10	The hashing/encryption algorithm of the proposed solution must be in compliant with Etisalat Afghanistan cryptographic requirements.		
3.11	Forgetting or resetting password function must support MFA mechanism using OTP or email for verification		
4	**Authentication**		
4.1	The proposed system shall not provide access without valid username and password.		
4.2	All user access to the proposed system shall support integration with industry Privilege account Management (PAM) solutions.		

No.	Description	Compliance (YES/NO/NA)	Comments
4.3	For public web applications, the proposed system supports and uses CAPTCHA or OTP to prevent against password attacks including but not limited to Dictionary Attack, Brute Force and Password Spraying mechanism.		
4.4	For mobile applications, the proposed system shall support and uses fingerprint authentication method		
4.5	The proposed system supports and uses secure authentication protocols, like Kerberos, LDAP-S, NTLM V2 and above, HTTPs (for web applications)		
4.6	The proposed system will not use insecure authentication protocols including but not limited to FTP, Telnet, NTLM v1, and HTTP (for web applications)		
4.7	The proposed system shall support session timeout settings		
4.8	The proposed solution shall support secure API architecture to integrate systems to exchange data were deemed necessary.		
4.9	The proposed solution shall support integration with Identity and Access Management solution (IAM) for user lifecycle management via standard APIs.		
4.10	The proposed solution must support LDAP and RADIUS authentication.		
5	**Authorization**		
5.1	The proposed solution shall support role-based and Rule Based access controls that includes access profiles or security matrix (i.e., Role Name VS. Access Permissions)		
5.2	The proposed system supports role-based / rule-based access permissions, i.e., Administrator, Operator, Viewer, User…		
6	**Software Security**		
6.1	The software development and testing will not run on the production systems and will be running in an isolated environment.		
6.2	The software source code will not include clear-text passwords.		
6.3	The software code will not include insecure protocols, like FTP, telnet ...etc.		
6.4	The software testing will not use live/production sensitive or PII data unless it's masked as per Etisalat Afghanistan's Cybersecurity Policies		
6.5	The proposed system enforces input and output validation to prevent Cyber-attacks including but not limited to SQL Injection, Buffer Overflow, XSS and SSRF…etc.		
6.6	For web portals, the proposed solution shall include all the security controls to prevent / protect the application against OWASP Top 10 security attacks and risks		
6.7	For mobile application, the proposed system shall include security checks / controls to protect from mobile attacks, like SSL Pinning, Jailbreak, Anti-debug, Anti-hooking, and		

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

No.	Description	Compliance (YES/NO/NA)	Comments
7	**Security Event Logging**		
7.1	Proposed systems shall support standard logging protocols such as CIFS/Syslog/CSV logs files		
7.2	The system shall generate and support audit logs that contain the following fields (as a minimum): a) Username b) Timestamp (Date & Time). c) Source and Destination IPs d) Transaction ID & session information e) Failed/Successful Logins f) Modification of Security Settings g) Privilege Escalation h) User Account Modification		
7.3	The proposed solution shall support the integration with Etisalat Afghanistan NTP server for time synchronization and accurate logging.		
7.4	The proposed solution shall support integration with IBM QRadar for Log Aggregation and Correlation.		
8	**Public Cloud Security**		
8.1	Etisalat customers' and staff personal data (PII: name, contacts, address, Emirates ID, Passport number, Nationality …) is encrypted at rest and in transit using a strong industry-standard encryption protocol in full compliance with Etisalat Afghanistan's Cryptographic requirements.		
8.2	The Public Cloud setup that stores PII information shall be hosted in the UAE		
8.3	The Public Cloud setup is hosted in a dedicated tenant for Etisalat Afghanistan (i.e., not shared)		
8.4	The Public Cloud data center shall not be moved to another country or location without prior coordination and approval from Etisalat Afghanistan Cybersecurity Department		
8.5	All Etisalat data will be permanently erased from the Public Cloud on termination of the service or support agreement		
8.6	The proposed Cloud system supports Etisalat Afghanistan's Cloud Access Security Broker (such as Microsoft MCAS, Netskope CASB)		
9	**Virtualization and Container Security**		
9.1	If applicable, Bidder shall ensure the proposed virtualized infrastructure, service based and micro services architecture to support multi tenancy, zoning & micro-segmentation, security visibility, secure virtualization (sVirt), trusted image signing, virtual Firewalls, DoS protection, Trusted platform module (TPM), Hypervisor & Host OS security to secure data and resources.		
9.2	The proposed solution shall support integration with Etisalat/Leading Container Security Solution, where		

No.	Description	Compliance (YES/NO/NA)	Comments
	applicable, to scan the container images and ensure malware protection of CI/CD pipeline.		
10	**Artificial Intelligence and Machine Learning Security**		
10.1	If the proposed solution uses AI/ML, it must ensure model integrity, prevent model poisoning, and protect training data from leakage.		
10.2	Any AI model must be explainable and auditable, especially for systems impacting customer services or security decisions		
10.3	AI/ML-based systems must include monitoring to detect adversarial inputs or behavioral drift.		
10.4	Access to AI training datasets must be role-based and logged.		
11	**Encryption and Key Management**		
11.1	All sensitive data at rest and in transit must be encrypted using strong encryption standards (AES-256, TLS 1.3, etc.).		
11.2	Key management must be handled via secure KMS (Key Management Systems) in compliance with Etisalat Afghanistan's Cryptographic Policy.		
11.3	Private keys and credentials must not be hardcoded into applications or scripts.		
12	**Database Security**		
12.1	The database must enforce the least privilege of access and role separation.		
12.2	Database activity monitoring (DAM) should be enabled and integrated with the SIEM.		
12.3	Sensitive fields (e.g., PII, financials) must be encrypted and masking enabled for non-privileged users.		
12.4	Default accounts and unused stored procedures must be disabled or removed.		
13	**Network Security**		
13.1	The solution must comply with Etisalat Afghanistan's network segmentation and zero trust architecture.		
13.2	2 All network connections must be protected using firewalls, IDS/IPS, and NDR (Network Detection and Response).		
13.3	Insecure protocols (e.g., Telnet, SMBv1) must be disabled.		
13.4	Remote access must be restricted and controlled through VPN, MFA, and PAM.		
14	**API Security**		
14.1	APIs must enforce authentication and authorization using OAuth2.0 or JWT standards.		
14.2	APIs must be protected against OWASP API Top 10 vulnerabilities.		
14.3	API traffic must be logged and monitored with anomaly detection.		

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

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	

==========End of Document ==========