TENDER NOTICE

No. EA/02-04-2026

For Campaign Management / Customer Value Management (CVM) Solution

1. Proposals are invited from companies of repute or their authorized agents for **"Campaign Management / Customer Value Management (CVM) Solution"**, according to Etisalat Afghanistan Scope of Work as per RFP.
2. Proposal can be submitted/shared through email to ghurzang@etisalat.af by 21 January 2026. Please clearly indicate **"Campaign Management / Customer Value Management (CVM) Solution,"** on the subject line of your email.
3. **Vendors must submit their proposals using an email subject line that exactly matches the RFP title as stated in this document. Etisalat will not be responsible for the missed proposals due to incorrect subject lines.**
4. You may also download this Bid Document from the Etisalat Afghanistan website at: www.etisalat.af/en/about-us/doing-business-with-us/tenders
5. Offer received after the above deadline shall not be accepted.
6. **The vendor shall submit the proposal in two separate parts: Technical and Commercial. The Commercial part must be submitted as a password-protected soft copy. The password will be requested once the evaluation committee begins the commercial evaluation of the bids.**
7. The vendor must demonstrate relevant experience in providing training services like those requested by Etisalat Afghanistan. Interested vendors are required to provide and share supporting documents that verify their expertise and past performance in this field. These documents should be submitted along with the proposal for evaluation purposes.
8. Etisalat Afghanistan reserves the full discretion to accept or reject any or all bids and to cancel the bidding process at any stage, without incurring any liability to the bidders or any obligation to provide reasons or notify the affected bidders of the decision.
9. All correspondence regarding this matter should be directed at:

Ghurzang Waziri
Assistant Manager, Procurement and Contracts
Email: ghurzang@etisalat.af
Contact No: +93781204068

Please also copy Mr. Ihsanullah Zirak, Director of Procurement & Supply Chain, at Ihsanullah@etisalat.af

Request for Proposal
(RFP)

For

Campaign Management / Customer Value Management (CVM) Solution

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 can attain the Performance Level specified in the Technical Specifications in accordance with the provisions of the Contract.

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

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

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

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

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

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

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

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

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

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

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

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

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

"Day" means calendar day of the Gregorian calendar.

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

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

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

"Etisalat Afghanistan (EA)" means the company registered under the Laws of Islamic 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 contractor in writing.

"Final Acceptance Certificate" means the certificate issued by EA after successful completion of warranty and removal of defects as intimated by EA.

"Force Majeure" means Acts of God, Government restrictions, financial hardships, war and hostilities, invasion, act of foreign enemies, rebellion, revolution, riot, industrial disputes, commotion, natural disasters and other similar risks that are outside of Contractor's and EA's control.

"Goods Receipt Certificate" means certificate issued by the consignee certifying receipt of Goods in good order and condition.

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

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

"Month" means calendar month of the Gregorian calendar.

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

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

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

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

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

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

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

2. INTRODUCTION TO WORK.

2.1 Bids are invited for Campaign Management / Customer Value Management (CVM) Solution accordance with Etisalat specifications and Annexures.

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 Purchaser in the Tender documents.

4. Price and Payment Term

4.1 Payment shall be made by bank transfer after receipt of original Hardcopy of invoice.

4.2 Advance payment shall not be made to the contractor.

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

4.4 Payments are subject to deduction of income tax at the prevalent rate from the relevant invoices of the contractor and paid to the Tax Authorities, except those especially exempted by the authorities. EA will issue a certificate of deductions to the contractor to enable him to settle tax returns with the concerned authorities.

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

4.5.1 For Supply of Equipment (Hardware & Software);

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

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

4.5.2 For Installation, Testing, Commissioning and Professional Services (if available).

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

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

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

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

5. Liquidated Damages Clause:

In order to ensure timely performance, the Contractor shall be liable to pay liquidated damages to EA for any delays in meeting the milestones or deliverables as defined in the Contract, provided such delays are attributable to the Contractor's fault.

Liquidated damages shall be calculated at a rate of one percent (1%) per week of the total value of the delayed portion of the Contract, up to a maximum of ten percent (10%) of the value of the affected portion.

If the maximum limit is reached, EA reserves the right to terminate the Contract without prejudice to any other remedies available under the Contract or applicable law.

6. Construction of Contract:

The Contract shall he 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.

7. Termination of the Contract

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

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

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

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

8. Local Taxes, Dues and Levies:

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

8.2 Withholding tax (if applicable) shall be deducted on local portion only as per prevailing rates as notified Islamic Emirate of Afghanistan. The amount of withholding Tax(s) is 2% of all project cost for local/registered companies who have Afghanistan Government Official Work License and 7% for International/ nonregistered companies.

9. Force Majeure

9.1 The contractor 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.

9.2 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 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 One (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.

9.3 If a Force Majeure situation arises, the contractor 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 fulfil its obligations under the contract as it is reasonably practicable and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.

10. Annexures:

The annexures listed below form an integral part of this RFP

Annexure- A..... Scope of Work

Annexure- B..... Cybersecurity Requirements

Annexure- C..... Supplier Code of Ethical Conduct.

Annexure –D ..... Compliance Clauses.

Annexure –E ..... Non-Disclosure Agreement (NDA)

Annexure –F ..... General Terms Compliance and Bidder Contact Details

Annexure-A

SCOPE OF WORK (SoW)

Campaign Management / Customer Value Management (CVM) Solution

Introduction

Etisalat Afghanistan seeks to procure a comprehensive Campaign Management and Customer Value Management (CVM) solution that enables deep analytical insights, automated journeys, AI/ML-driven personalization, and enhanced customer lifecycle management. The purpose of this SoW is to define the scope, deliverables, responsibilities, timelines, and governance structure for the selected vendor.

Objectives

- Deploying an enterprise-grade CVM platform
- Implement a unified Customer Data Platform (CDP)
- Enhance automation, segmentation, and offer personalization
- Reduce churn and improve ARPU uplift
- Build internal capability across Commercial, RA, and IT teams

Scope of Work

The solution must include Full Platform Setup, CDP implementation, Campaign Management, AI/ML model deployment, Integrations, Reporting, and a Validation & Governance Framework.

Technical Requirements

A. Platform Requirements

- High availability architecture
  - Active-Standby/PR-DR/Redundant systems and failover capabilities to ensure continuous operation.
  - Load balancing for optimal resource allocation and performance.
- Real-time campaign execution
  - Immediate processing and deployment of campaigns based on live data.
  - Support for real-time decision-making during customer interactions.
- Drag-and-drop journey builder
  - User-friendly interface to create and modify customer journeys without coding.
  - Pre-built templates to expedite the design process.

B. CDP Requirements

- Unified data ingestion (real-time + batch)
- Identity resolution (User Profiling)
- Event-based triggers

C. Integrations

- API Support

  Well-documented API endpoints or support for ease of use and developer onboarding.
  - Versioning of APIs to ensure backward compatibility and smooth updates.
- Capability to integrate with upstream and downstream but not limited to below CVBS/DWH/App/USSD/SMSC/MFS/IVR/Social/etc.
- Real-Time Data Syncing:
  - A mechanism for consistent data updates across integrated systems. In case of any failure in data fetching or uploading, an automatic alert should be generated.
- Adaptable Transformation Framework:
  - Built in tools to transform data format and reconcile discrepancies across different systems.
  - Support for mapping fields from various data sources to a unified customer schema.

D. AI/ML Capabilities

- Prebuilt models + custom model training
- Monitoring dashboards

E. Security Requirements

- Encryption in transit & at rest
- Full audit trails
- Integration with EA SIEM solution
- Implementation of MFA for web portal
- Support for EA EDR solution installation
- Support for EA Temable agent installation for vulnerability scan
- Enforcement of Password policies & session timeout standards
- LDAP/AD integration
- Integration with EA Identity & Access Management

F. Data Warehouse Integration:

- The Solution shall integrate natively with Etisalat Afghanistan's Enterprise Data Warehouse, which is the central source of truth for customer, usage, product, revenue and network data.
- All required input data for the Solution (including but not limited to PAYG usage, bundles, SMS, VAS, interconnect, customer and product master data) shall be sourced from EDW through agreed interfaces (batch files, database views, APIs or ETL jobs), as defined jointly with the EDW team.
- The Solution should also provide outbound data feeds back to EDW via db link and SFTP to provide well formatted output in the CSV files or database format, including:

    - Campaign definitions and execution logs
    - Segmentation results and scoring outputs
    - Response, uplift and revenue attribution KPIs
    - Any additional analytical datasets required by Commercial, Finance or BI teams.
- Integration frequency (near real-time, hourly, daily) and SLAs for each data feed shall be defined during the design phase, and the Solution must support these SLAs without performance degradation.
- The Vendor shall deliver full technical specifications for all inbound and outbound data interfaces with EDW (file layouts, APIs, data models, transformation rules, error handling and reconciliation logic).
- All EDW integrations shall comply with Etisalat Afghanistan's information security policies, including secure connectivity, access control, data masking (where applicable) and logging of all data movements.

Risk Assessment

Identified Risks:

- Delayed integrations
- Data inconsistencies
- Financial and opportunity Loss
- Resource availability

constraints Mitigations:

- Weekly governance meetings
- Pre, during and post validation tests
- Fallback plans & contingency cycles

End-to-End CVM Flows

A. Data Flow

- Source Systems generate events and records (CDR, CVBS, App, USSD, DWH, Complaints/CC, Digital).
- Data is ingested into the CDP in real-time and batch modes (via APIs, streams, and scheduled ETL jobs).
- CDP performs identity resolution (Profiling), cleansing, and enrichment to build 360° customer profiles.
- Processed and standardized customer attributes are exposed to the CVM engine for segmentation and targeting.
- Aggregated KPIs and model scores are computed and refreshed based on agreed frequencies.

- Downstream dashboards and reports consume the curated data from CDP/CVM for decision-making.

B. Campaign Lifecycle Flow

- Business Need Definition: Commercial defines campaign objectives, target segments, and success KPIs.
- Segment Design: CVM/Analytics team defines eligibility rules, rule-based exclusions, and frequency caps/exclusions.
- Segment Validation: Sample MSISDNs are validated jointly with CVM/RA/IT/DWH before activation.
- Journey Design: Campaign journeys (single wave, multi-wave, trigger-based) are configured in the CVM tool.
- Channel Mapping: Channels (SMS, USSD, App, IVR, Social etc.) are selected and configured.
- Offer & Provisioning Rules: Charging and provisioning logic is integrated with CVBS and other systems.
- Testing: End-to-end test with a small test group is executed and validated on Test Bed.
- Launch: Campaign is launched according to business calendar, with monitoring in near-real-time.
- Optimization: Based on performance insights, offers, creatives and segments are fine-tuned (A/B testing).
- Closure & Post-Analysis: Post-campaign evaluation is conducted, including uplift, ROI, and learning points.

C. Segment Validation & Governance Flow

- Monthly CVM Governance Committee meeting is scheduled with CVM Team and other stakeholders.
- For each active campaign/segment, a random sample (e.g., 1,000 MSISDNs) is extracted from the tool.
- Pre-behavior and eligibility checks are performed by CVM and RA to confirm correct targeting.
- Any anomalies (e.g., non-eligible, repeated benefits) are logged, and root causes are investigated with IT/vendor.
- Corrective actions are implemented (rule changes, exclusion lists, fixes in logic, etc.).
- Updated rules and lessons learned are documented and shared for future segment design.
- Summary of decisions and outcomes are recorded in governance minutes and tracked over time.

Detailed Requirements

1. Functional Requirements

- Ability to design and execute multi-step customer journeys across multiple channels.
- Support for static, dynamic, propensity-based, and event-triggered segments.
- Capability to define eligibility, exclusion, and frequency capping rules at customer and campaign level.
- Support for A/B testing, control groups, and automated hold-out groups for uplift measurement.
- Real-time decisioning and event-based triggering (e.g., recharge event, App activity, usage drop, inactivity, SIM reactivation, etc.).
- Support for inbound and outbound use cases (e.g., triggered offer on App/USSD, scheduled outbound SMS).
- Campaign cloning, reusability of segment definitions, and centralized library of rules and journeys.
- Customizable dashboards for campaign, segment, and performance monitoring.
- The platform shall be able to support standard languages including Pashto and Dari local languages.
- The Platform shall be able to implement the standard Communication Policy of limiting number of SMS a user can get in a period i.e. day, as well as limit the communication time i.e. 7AM – 6PM.

2. Data & CDP Requirements

- Support ingestion from multiple data sources: CVBS, DWH, Network, App, USSD, Complaints/CC, digital, and third-party feeds.
- Real-time event ingestion (e.g., via streaming platform or APIs) and batch loads (via ETL).
- Customer identity resolution using MSISDN, e-NID, device, and other keys where applicable.
- Historical data and logs storage to support long-term behavioural modelling (at least 6 months of history).
- Ability to define and compute derived attributes and KPIs (e.g., RGS, ARPU, DoU, MoU, recharge patterns).
- Data quality checks and alerts (missing data, delayed files, schema changes).

3. Integration Requirements

- Standard APIs for inbound and outbound interactions with external systems.
- Integration with CVBS for real-time eligibility checks and provisioning of offers.
- Integration with SMSC, USSD Gateway, Mobile App, Social, IVR, and other channels.
- Secure connectivity to DWH/Big Data platforms for advanced analytics and reporting.
- Ability to consume scores and outputs from external models as well as exposing scores to other systems.

- Clear API documentation, including error codes, rate limits, payload formats, and security mechanisms.

4. Security & Compliance Requirements

- Role-based access control (RBAC) with the ability to define granular permissions for users and groups.
- Comprehensive audit logging of user activities, configuration changes, and campaign executions.
- Encryption of data in transit and at rest in line with EA and regulatory standards.
- Support for segregated environments (Dev, UAT, Prod) and controlled promotion process.
- Compliance with ATRA and Etisalat Afghanistan's internal information security policies.

5. Performance & Scalability Requirements

- Ability to support millions of subscribers and high campaign volumes without performance degradation.
- Near real-time execution of event-based campaigns (e.g., under 2 seconds for decisioning where applicable).
- Scalability to handle peak loads, such as national promotions, emergency notifications, or regulatory broadcasts, not only through campaigns but also via bulk messages (A2P/P2A) with configurable sender IDs (e.g., 888, Etisalat, etc.) supporting Eng/Dari/Pashto languages and offering unlimited broadcasting (Single/batch) capabilities per day.
- System health monitoring with alerts and dashboards for key performance indicators (KPIs).

6. Operational & Support Requirements

- 24/7 support for critical incidents during and after go-live, as per agreed SLAs.
- Knowledge transfer and structured training for Commercial, RA, IT, and Analytics teams.
- Clear runbooks and SOPs for common operational tasks (campaign creation, roll- back, troubleshooting).
- Regular health checks, platform upgrades, and roadmap reviews with EA stakeholders.

Commercial Requirements and Use cases:

The objective is to procure an enterprise-grade solution that delivers advanced segmentation and data modelling, personalized engagement, real-time decisioning, and measurable

revenue uplift while offering full operational control to Commercial, CVM, and Analytics teams:

1. Performance Measurement & Analytics:
    a. Automated KPI reporting, uplift measurement, and incremental revenue analysis.
    b. Support for test/control groups, A/B testing, modeling techniques, and audience scoring.

2. Omnichannel Communication Integration:
    a. Seamless integration with SMS, USSD, App, Social, OBD/IVR, and digital channels.
    b. Capability to onboard new communication channels with minimal dependency.
3. Advanced Segmentation & Targeting:
    a. Real-time, dynamic, behavioral, and predictive segmentation capabilities.
    b. Automated validation, suppression/exclusion logic, and profiling of eligible audiences.

4. Campaign Orchestration & Journey Automation:
    a. Drag-and-drop journey builder with multi-step, multi-channel orchestration.
    b. Real-time triggers, eligibility checks, frequency capping, and offer prioritization.

5. Real-Time Decisioning & Personalization:
    a. Support for Next Best Action (NBA) and contextual offer recommendations.
    b. Instant access to customer profiles and low-latency event handling.

6. Integration & Data Linkage:
    a. Capability to connect to the 3rd parties but not limited to DWH, OCS/IN, CRM, loyalty systems, and real-time data feeds.
    b. Ability to create/consume structured tables and data pipelines.

7. Visualization & Insights:
    a. Executive dashboards for revenue, performance, and campaign insights.
    b. Visual workbench for campaign design and reporting

TG/CG Measurement (Overall & Campaign-Level)

1. TG/CG Measurement at Overall Level:
    a. The platform must provide enterprise-level TG/CG analytics, enabling Commercial and CVM teams to assess the overall incremental uplift driven by all combined campaigns.

b. It should automatically compute net and gross conversions, incremental revenue, ARPU uplift, and behavioral shifts across the entire targeted base versus the control population.
c. The system must allow executive dashboarding for overall TG/CG performance, enabling management to monitor the impact of CVM strategy on churn, reactivation, engagement, and revenue.

2. TG/CG Measurement at Campaign Level
   a. For each campaign, the platform must automatically define, measure, and report Target Group vs. Control Group outcomes to determine campaign- specific uplift.
   b. It should calculate KPIs such as take-rate, conversion rate, incremental revenue, usage uplift, retention uplift, and campaign ROI.
   c. The measurement must cover offer-level uplift, ensuring Commercial can compare offers, optimize performance, and refine future campaign mapping.
   d. Statistical significance checks and automated stratified random sampling must be supported to ensure accuracy

Business Objectives

Objective	Key Performance Indicator (KPI)	Target
Increasing Campaign ROI	Increase in campaign-generated revenue	10% increase within 12 months
Improve Customer Retention	Reduction in customer churn rate	15% reduction within 12 months
Enhance Customer Engagement	Increase in email open rates and click-through rates	20% increase within 6 months
Improve Cross-Sell and Upsell	Increase in the number of products per customer	10% increase within 12 months
Reduce Time-to-Market	Reduction in average time to launch a campaign	50% reduction within 6 months
Improve Customer Satisfaction	Increase in NPS score	5 points increase within 12 months
Increase Social Media Engagement	Growth in social media followers and engagement rate	30% increase within 12 months
Improve AI-Driven Insights	Percentage of campaigns using AI recommendations	20% of campaigns within 12 months

Additional Business Requirements

Functional requirement

Feature	Detailed Requirement
Approval Workflows	Multi-level approval workflows to ensure governance and compliance

Segmentation

Demographic Segmentation: Segment customers based on demographic attributes such as age, gender, location, and income level.
Behavioural Segmentation: Segment customers based on their behavior, including purchase history, service usage patterns, and engagement levels.
Psychographic Segmentation: Segment customers based on their attitudes, values, and lifestyle preferences.
RFM Analysis: Implement Recency, Frequency, and Monetary (RFM) analysis to identify high- value customers and at-risk customers.
Predictive Segmentation: Use machine learning to predict which customers are likely to churn, upgrade, or respond to specific offers.
Look-Alike Modelling: Identify new customers who are similar to our best customers.

Personalization

The CMS must provide comprehensive personalization capabilities that enable our marketing team to deliver tailored experiences to individual customers:
Content Personalization: The system must support dynamic content insertion, allowing different content to be shown to different customers based on their attributes and behaviour. Product recommendations should be personalized based on customer preferences and purchase history. Offers should be personalized based on customer value and propensity to purchase.
Channel Personalization: The system should intelligently select the optimal channel for each customer based on their communication preferences and historical engagement patterns. Journey Personalization: The system should enable the creation of personalized customer journeys that adapt based on customer behaviour and lifecycle stage. Different customers should receive different messages and offers based on their individual characteristics and needs.

Digital CVM

CVM Feature	Detailed Requirement
Customer Lifecycle Management	Tools for managing acquisition, onboarding, retention, and loyalty stages

Next Best Action Engine	AI-powered recommendations for optimal customer actions in real-time
Personalized Journeys	Multi-step customer journeys that adapt to behavior across channels
Customer Value Scoring	Scoring based on CLV, churn risk, and engagement metrics
Loyalty Program Integration	Support for tiered loyalty programs and reward management
Retention Campaigns	Automated campaigns to identify and retain at-risk customers

Social Media integration

Social Media Feature	Detailed Requirement
Social Listening	Monitor mentions, sentiment, and trends across major platforms
Social Campaign Management	Create, schedule, and publish content to multiple platforms
Content Calendar	Visual calendar for planning and managing social media content
Social Analytics	Track engagement, reach, impressions, and sentiment metrics
Community Management	Tools for managing customer interactions and responses
Influencer Management	Identify and manage relationships with relevant influencers
Sentiment Analysis	AI-powered analysis of customer sentiment and brand perception
Competitive Monitoring	Track competitor activity and messaging on social platforms

AI/ML capabilities

AI Capability	Detailed Requirement
Predictive Analytics	Predict churn, CLV, purchase propensity, and next product
Natural Language Processing	Analyze sentiment and extract insights from unstructured text
AI Recommendations	Personalized product and content recommendations in real-time

Anomaly Detection	Identify unusual patterns indicating fraud or churn risk
Customer Clustering	Unsupervised ML for identifying natural customer segments
Campaign Optimization	ML algorithms for optimizing timing, messaging, and offers
Churn Prediction	Identify at-risk customers and recommend retention actions
Propensity Modeling	Predict likelihood of purchase for specific products/services
Automated Insights	AI-generated insights and recommendations for marketers

Analytics & monitoring

Dashboards: Customizable dashboards should allow users to monitor key metrics such as campaign performance, customer engagement, and revenue impact. Dashboards should be configurable to show different metrics for different user roles.
Reports: The system should provide a library of pre-built reports covering common use cases such as campaign performance, customer segmentation, social media performance, and ROI analysis. Users should be able to create custom reports based on their specific needs.
Advanced Analytics: The system should provide advanced analytics capabilities including customer lifetime value (CLV) analysis, churn prediction, and attribution modeling. These capabilities should help us understand which marketing activities are driving the most value.

Performance and Scalability

Requirement	Metric
Scalability	Support 50% customer base growth over 3 years
Response Time	Less than 2 seconds for all user actions
Email Throughput	[Number] emails per hour
SMS Throughput	[Number] SMS messages per hour
Database Query Response	Less than 5 seconds for standard reports
Complex Query Response	Less than 30 seconds for analytical queries
API Response Time	Less than 500ms for 95th percentile requests

Technical Architecture

Key architectural requirements include:

Cloud-Based Deployment: The system should be deployed on a major cloud platform such as AWS, Azure, or Google Cloud. This ensures scalability, reliability, and security.
Microservices Architecture: The system should be built using microservices architecture, where different functional components are deployed as separate services. This enables independent scaling and deployment of different components.
API-First Design: The system should be designed with APIs as the primary interface, enabling integration with other systems and future extensibility.
Containerization: The system should use containerization (e.g., Docker) to ensure consistency across different environments and enable efficient resource utilization.
Load Balancing: The system should use load balancing to distribute traffic across multiple servers and ensure high availability.
AI/ML Infrastructure: The system should have a robust infrastructure for training and deploying machine learning models. This should include support for popular ML frameworks and tools

Implementation Plan

Core CMS Implementation (Month 1)
- System setup and configuration
- Data migration from legacy systems
- Integration with CRM and billing systems
- Basic campaign management capabilities
- User training and go-live support

Advanced Analytics, Personalization, and Digital CVM (Months 2)
- Implementation of predictive analytics capabilities
- Machine learning model development
- Advanced personalization rules
- Customer journey orchestration
- Digital CVM capabilities including next best action engine
- Advanced reporting and dashboards

Social Media Integration and AI Capabilities (Months 1)
- Integration with social media platforms
- Social listening and monitoring capabilities
- Social media campaign management
- Advanced AI capabilities including NLP and sentiment analysis
- Performance optimization
- Ongoing support and optimization

Annexure-B

Cybersecurity Requirements

General Security Requirements:

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

- Date and time of activity
- Source and Destination IP for the related activity
- Identification of user performing activity
- Description of an attempted or completed activity.

20. The system must support live log retention of 1 Year and backup up to 3 years.
21. System must be capable of encrypting the log files to ensure user does not modify or change the logs.
22. System must provide cryptographic algorithms such as AES 128/256 Bit, SHA 256/384/512 bits.
23. System must be secure against well-known attacks including but not limited to SQL Injection, XSS, CSRF, SSRF, Code Execution and other attacks.
24. Vendor system's password configuration must be aligned with EA Information security policies.
25. System must support integration with LDAP, IAM "Identity and Access Management" and PAM "Privileged Access Management" Solutions.
26. System must support external log synchronization mechanisms to push logs to another system for analysis such as SIEM and centralized log server.
27. The database must support the encryption of admin user's information with algorithms such as PBKDF2 and SHA256/384/512 bits.
28. The database platforms "if any" must support the encryption of data in-transit and at rest.

Important Note:

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

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

S/N	Description	Compliance (YES/NO/NA)	Comments
	security standards or best security practices, before the new product or any of its releases is delivered to ETISALAT. The Contractor/Supplier/vendor shall provide evidence/report of the security assessment/audit of the proposed solution.		
2	Security Architecture		
2.1	The Contractor/Supplier/vendor shall ensure that proposed solution shall comply with the applicable IT and Telecom Security standards (such as Afg. NESA (SIA) IA V2, Afg. DESC (ISR), Afg. TRA, 3GPP, ETSI, ENISA, CSA, NIST, PCI, ISO, GDPR etc.) The Contractor/Supplier/vendor shall confirm the applicable standard.		
2.2	The proposed solution shall support the latest operating systems and application versions. Contractor/Supplier/vendor to ensure proposed solutions will run the latest stable software, operating system, and firmware.		
2.3	The solution shall be designed with multi-tier architecture, (Demilitarized Zone (DMZ), middleware, and private network). Any system accessible from the Internet shall be on the DMZ and access to internal sensitive data shall be secured through the middle tier application proxy.		
2.4	The proposed solution shall not impact or relax existing Etisalat security control or posture.		
2.5	The performance of the proposed system shall meet the business requirements without disabling or removing any existing security control		
2.6	The Contractor/Supplier/vendor shall provide only secure methods of communication such as HTTPS, SFTP, SCP, TLS1.3, IPSEC, SRTP, SSH v2, SNMPv3 between the proposed nodes. Non-secure protocols such as Telnet, HTTP and FTP shall not be used.		
3	Password Security		
3.1	All Operating Systems (e.g. Linux and Windows) shall be hardened according to well-known standards such as, but not limited to NIST, CIS security benchmark, and NSA.		
3.2	The proposed system includes password management module that supports the following features:		
3.3	Setting the minimum password length		
3.4	Password complexity, and not accepting blank		

S/N	Description	Compliance (YES/NO/NA)	Comments
	passwords		
3.5	Maximum password age and password history		
3.6	Account lockout		
3.7	Enforce changing password after first login		
3.8	Prompt / notify for the old password on password changes		
3.9	The password shall be saved in hashed format (i.e. irreversible encryption)		
3.10	Forgetting or resetting password function shall support using OTP or email for verification		
4	Authentication		
4.1	The proposed system shall not provide access without valid username and password.		
4.2	All user access to the proposed system shall support Privilege account Management (PAM) integration.		
4.3	For public web applications, the proposed system supports and uses CAPTCHA or OTP to prevent password dictionary attacks		
4.4	For mobile applications, the proposed system shall support and uses fingerprint authentication method		
4.5	The proposed system supports and uses secure authentication protocols, like Kerberos, LDAP-S, NTLM V2 and above, HTTPs (for web applications)		
4.6	The proposed system will not use insecure authentication protocols, like NTLM v1, HTTP (for web applications)		
4.7	The proposed system shall support session timeout settings		
4.8	The proposed solution shall support secure API architecture to integrate systems to exchange data where deemed necessary.		
5	Authorization		
5.1	The proposed solution shall support role-based access controls that includes access profiles or security matrix (i.e. Role Name VS. Access Permissions)		
5.2	The proposed system supports role-based access permissions, i.e. Administrator, Operator, Viewer, User…		
6	Software Security		
6.1	The software development and testing will not run on the production systems, and will be running in an isolated environment		
6.2	The software source code will not include clear-text		

S/N	Description	Compliance (YES/NO/NA)	Comments
	passwords		
6.3	The software code will not include insecure protocols, like FTP, telnet ...etc.		
6.4	The software testing will not use live/production sensitive or PII data unless it's masked as Etisalat security policy		
6.5	The proposed system enforces input and output validation to prevent security attacks, like SQL Injection, Buffer Overflow...etc.		
6.6	For web portals, the proposed system includes all security controls to prevent/protect from OWASP Top 10 security attacks and risks		
6.7	For mobile application, the proposed system shall include security checks / controls to protect from mobile attacks, like SSL Pinning, Jailbreak, Anti-debug, Anti-hooking, and Advanced Obfuscation...		

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

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

Annexure-C

Code of Ethical Conduct

Content

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, contractors, subcontractors, 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 subcontractors 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-contractors.

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 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 Labour, and Human Trafficking

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

6.2. Etisalat Afghanistan prohibits the use forced labor, whether in the form of prison labor, indentured labor, bonded labor 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 labor, slavery, or human trafficking. We will treat any reported incidents seriously, with respect and confidence.

6.3. Etisalat Afghanistan condemns all forms of exploitation of children. We remain committed to prohibit and eliminate the use of child Labor 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

labor 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 employees' 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 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 color, 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, contractors and sub-contractors 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 program, 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, contractors, 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, minimizing, 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-contractors when undertaking any work or activities on behalf of Etisalat Afghanistan.

10.4. Summary of HSE (Health, Safety and Environment) terms and conditions for contractors:

- Contractors, 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.

- 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.

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

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

-Contractor 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.

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. Suppliers shall minimize 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 behavior 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 subcontractors working on the Supplier's behalf for Etisalat Afghanistan: via the official Etisalat Afghanistan whistle-blower email eawb@etisalat.af.

Annexure-D

Compliance Clauses

1. Anti-Bribery Anti-Corruption

1.1 The Contractor 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, contractors, sub-contractors 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 ("**Relevant Requirements**") to the extent applicable to the Parties, and related laws and regulations of Afghanistan.

(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 Contractor 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 Contractor 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 Contractor 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 Contractor or acquires a direct or indirect interest in the Contractor and the Contractor 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 Contractor 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 Contractor 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 Contractor shall ensure that any third party associated with the Contractor 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 Contractor in this [Annex 1]. The Contractor 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 Contractor includes any subcontractor of the Contractor. The Contractor may only engage a third-party (e.g., subcontractor) 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 Contractor 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 Contractor's compliance with this [Annex 1], and the Contractor warrants its full cooperation with any investigation of suspected violations, including but not limited to, the timely provision of all relevant information, records, documentation, evidence, and employees, as may be requested by [Etisalat Afghanistan].

3.4 [Etisalat Afghanistan] shall be entitled to suspend payments of Contractor invoices that are, or become due in case there is a reasonable believe that the Contractor 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 Contractor 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

[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.*

Contractor.

3.6 Breach of this [Annex 1] shall constitute a material breach of this Agreement by the Contractor. If the Contractor 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 Contractor 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 Contractor or same owner(s) and/or or agents, suppliers or other contractors of the Contractor.
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 Contractor 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 Contractor, 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 Contractor including, without limitation, agents, contractors, sub-contractors 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 Contractor 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 Contractor 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 Contractor represents, warrants and undertakes that:

2.1 Neither the Contractor, 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 Contractor 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 Contractor will not cause [Etisalat Afghanistan] to violate any Applicable Sanctions/Export Control Laws.

2.4 The Contractor 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 Contractor 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 Contractor shall notify [Etisalat Afghanistan] in writing as soon as possible if:
(i) The Contractor, 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 Contractor, 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 Contractor 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 Contractor, 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 Contractor during the period of any such audit. Contractor, 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 Contractor agrees that non-compliance with any of the representations and/or obligations set out in this Agreement by the Contractor, 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 Contractor for cause without liability as specified in the Agreement.
8. The Contractor 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 Contractor, 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 Contractor 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 Contractor, 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 Contractor, 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 Contractor shall provide such assistance to [Etisalat Afghanistan] in obtaining such approval as [Etisalat Afghanistan] may reasonably require.

2. 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 Contractor, that prohibit engaging in or facilitating financial transactions that promote or conceal unlawful activity in any jurisdiction.
2. The Contractor represents and warrants that:

i. the Contractor 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 Contractor has in place procedures aimed at preventing AML/CFT violations; and
iii. the Contractor 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-E

NON-DISCLOSURE AGREEMENT (NDA)

Etisalat Afghanistan, a telecommunication company incorporated under the laws of Islamic Emirates of Afghanistan having its principal office at IHSAN Plaza, Char Rahi Haji Yaqoub, Shar-e-Now, PO Box No.800, Kabul, Afghanistan (hereinafter called "Etisalat") which expression where the context so permit shall mean and include its assigns, administrators and successor on the other part.

And

Vendor,.....

(Both hereafters individually referred to as the "Party" and jointly referred to as the "Parties").

IN CONSIDERATION of the promises and mutual covenants and obligations contained herein IT IS HEREBY AGREED as follows:

1. For the purposes of this Mutual Non-Disclosure Agreement (this "Agreement"):

   (a) "Business Purpose" means: (i) assessing the desirability or viability of establishing or furthering a business or contractual relationship between Parties; and (ii) to the extent this Agreement is incorporated by reference into any other agreement between the Parties, achieving the objectives of that agreement.

   (b) "Confidential Information" means all information provided by the Disclosing Party (hereinafter defined), whether commercial, financial, technical or otherwise (including, without limitation, business information/ models, names of customers or partners (whether potential or existing), proposed business deals, corporate strategies, cost and pricing data, market and/ or financial projections, ideas, discoveries, inventions, specifications, formulae, programs, plans, drawings, models, samples, requirements, standards, presentations, software and supporting documentation, trade- and manufacturing and know-how secrets), disclosed to the Receiving Party (hereinafter defined), in connection with the Business Purpose, (whether disclosed orally, in documentary form, by demonstration or otherwise) (i) which is contained in any form whatsoever (including without limitation data, drawings, films, documents and computer readable media) and (ii) which is marked or otherwise designated to show expressly or by necessary implication that it is confidential or proprietary or which is inherently of a confidential or proprietary nature, together with notes, analyses, work papers, compilations, comparisons, studies or other documents prepared by either party which contain, reflect or are based on or generated from such Confidential Information.

   (c) "Disclosing Party" means the party disclosing the Confidential Information.

   (d) "Members of the Receiving Party's Group" means, if the Receiving Party's employees, shareholders, dealers, distributors, board, advisors, auditors, sub-contractors, subsidiaries and affiliates; and if the Receiving Party is one of the Suppliers: any person, now or hereafter existing, who directly or indirectly controls, is controlled or is under common control with one of the Suppliers; a

person "controls" another person if it holds or is beneficially entitled to hold, directly or indirectly, other than by way of security interest only, more than fifty percent (50%) of its voting rights, income or capital.

(e) "**Receiving Party**" means the party receiving the Confidential Information.

(f) "**Disclosure Period**" means this Agreement applies to Confidential Information disclosed between the Effective Date or the first date Confidential Information is disclosed by the Disclosing Party to the Receiving Party, whichever comes first, and three (3) years thereafter.

(g) "**Confidentiality Period**" means the Receiving Party's duties with respect to Confidential Information under this Agreement and such duties shall expire five (5) years from the date of its disclosure hereunder (except trade secrets, which shall remain subject to the terms of this Agreement for so long as they constitute trade secrets).

2. Each party warrants in respect of Confidential Information for which it is the Receiving Party:

(a) To treat Confidential Information as confidential during the Confidential Period;

(b) not to, without the Disclosing Party's prior written consent in each case, communicate, disseminate or disclose any part of such Confidential Information to any person except:

(i) Only to Members of the Receiving Party's Group; and

(ii) Where the Receiving Party is ordered by a court of competent jurisdiction to do so or there is a statutory obligation to do so except that such disclosure shall not be made without first timely informing the Disclosing Party in writing of the court order or statutory obligation and of the measures necessary to comply or dispute the same;

(c) To ensure that all persons and bodies mentioned in paragraph (b) (i) above are made aware, prior to the disclosure of such Confidential Information, of the confidential nature thereof, that they owe a duty of confidence to the Disclosing Party and agree to hold such Confidential Information in confidence in accordance with the terms of this Agreement; and to use its reasonable efforts to ensure that such persons and bodies comply with such obligations;

(d) Not to use or circulate such Confidential Information within its own organization except solely to the extent necessary for the Business Purpose or any other purpose the Disclosing Party may hereafter expressly authorize in writing; and

(e) To use all reasonable efforts to effect and maintain adequate security measures to safeguard such Confidential Information from unauthorized access, use and misappropriation.

3. The obligations of confidentiality in Clause 2 above shall not apply:

(a) To any portion of Confidential Information where the Receiving Party can demonstrate that the Confidential Information concerned is:

(i) Or has become publicly known through no fault of the Members of the Receiving Party's Group; or

(ii) Lawfully received from an independent third party without any restriction and without any obligation of confidentiality; or

(iii) Already known to the Receiving Party with no obligation of confidentiality at the date it was disclosed by or obtained from the Disclosing Party; or

(iv) Disclosed without restriction by the Disclosing Party to any third party *provided* that such third party is not a Member of the Receiving Party's Group.

(b) To any information which is independently developed by the Receiving Party without access to, use of or reference to the Disclosing Party's Confidential Information.

4. If only a portion of any Confidential Information falls within one or more of the exceptions in Clause 3, the remainder shall however continue to be subject to the prohibitions and restrictions set out in this Agreement.

5. All Confidential Information shall be and remain the property of the Disclosing Party and except as necessary for the Business Purpose shall not be reproduced in whole or part without the Disclosing Party's express written consent. Any copies of the Confidential Information shall become the Disclosing Party's property and shall contain any copyright and other proprietary rights notice or legend as appears on the original copy.

6. Nothing contained in this Agreement shall be construed as granting to or conferring on the Receiving Party any rights by license or otherwise, expressly or impliedly, for any invention, discovery or improvement made, conceived or acquired prior to or after the date of this Agreement relating to the Confidential Information of the Disclosing Party.

7. Nothing in this Agreement shall imply or create any exclusive relationship between the Parties. The Parties agree that the provision of Confidential Information hereunder and any discussions held in connection with the Business Purpose shall not prevent either Party from pursuing similar or other discussions with third parties provided that no breach of this Agreement is so occasioned or oblige that Party to take, continue or forego any action relating to the Business Purpose. Any estimates, forecasts or similar material provided by either Party to the other shall not constitute any commitments.

8. Upon the written request by the Disclosing Party, the Receiving Party shall promptly deliver to the Disclosing Party all the Disclosing Party's Confidential Information supplied to the Receiving Party and all copies thereof or destroy or erase all such Confidential Information contained in any materials and documentation or recorded in any memory device. Within fourteen (14) days of such request, an officer of the Receiving Party shall certify in writing to the Disclosing Party that it has fully complied with its obligations under this Clause.

9. Neither Party shall make or permit others to make any reference to the subject matter of this Agreement, to the Confidential Information, to the fact that Confidential Information was made available, that it has inspected any portion of the Confidential Information or use the name of the other party or any trademark of the same in any public announcements, promotional, marketing, sales materials or efforts without the prior written consent of the other party.

10. Regardless of the date stated on this Agreement, this Agreement becomes

effective as of the first date any Confidential Information of a Disclosing Party is made available to a Receiving Party.

11. Nothing in this Agreement is intended to confer any benefit on any third party or any right to enforce any term of this Agreement.

12. The termination of this Agreement or the completion of the Business Purpose for any reason shall not affect the obligations set out in this Agreement.

13 Any failure or delay in exercising any rights, power or privilege hereunder will not operate as a waiver thereof, nor will any single or partial exercise preclude any other further exercise thereof.

14 This Agreement shall be binding upon the Parties hereto and their respective successors, subsidiaries and affiliates. This Agreement is personal to the parties and may not be assigned or transferred by either party without the prior written consent of the other party.

15 The parties acknowledge that money damages may not be a sufficient remedy for any breach or threatened breach of this Agreement by a party and that the other party will be entitled to seek specific performance and injunctive relief as remedies for any such breach. Such remedies will be in addition to any other remedies available.

16 If any provision of this Agreement is held to be invalid or unenforceable in whole or in part, such invalidity or unenforceability shall attach only to such provision or part thereof and the remaining part of such provision and all other provisions hereof shall continue in full force and effect.

17 The construction, validity, performance or interpretation of this Agreement is exclusively governed by the laws of Islamic Emirates of Afghanistan.

18 Any dispute arising in connection with or out of the construction, validity, performance or the interpretation of this Agreement, which the parties cannot settle amicably, shall be finally settled by the sole jurisdiction of Islamic Emirates of Afghanistan courts.

19 This Agreement represents the entire agreement between the parties and supersedes and cancels all previous negotiations, agreements or commitments (whether written or oral) with respect to the subject matter hereof. This Agreement shall not be amended or modified in any manner, except by an instrument in writing signed by a duly authorized representative of each of the parties hereto.

20 The parties agree to treat documents sent via telephonic facsimile as original documents, provided that either party may require the other to provide a manually executed or authenticated original or duplicate of any document so sent within a reasonable period of time, and if such original or duplicate is not provided within that time, then to treat the document as not having been received initially until the manually executed or authenticated original or duplicate is delivered.

21 This Agreement is executed in duplicate original, either of which may be deemed the original, but together constituting only one agreement, and if executed at different times and/ or places, neither party shall be liable to the other party under this Agreement until receipt of the duplicate-original executed by the other party.

The Parties hereto agree to perform their obligations hereunder without any charge or expenses to each other.

IN WITNESS WHEREOF, the Parties have entered into this Mutual Non-Disclosure Agreement, effective as of the date first set forth above.

Annexure-F

RFP General Terms Compliance to be filled by Bidder.

S/N	Clause No. and General Terms	Comply (Yes/No)	Remarks
1	Validity of Offer		
2	Acceptance of Offers		
3	Payments		
4	Liquidated Damages Clause		
5	Construction of Contract		
6	Termination of the Contract by the Purchaser		
7	Local Taxes, Dues and Levies		
8	All Annexures including NDA		

The following Information must be submitted with offer.

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

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