CONTEU Token AML/CFT Policy Framework (FATF-Compliant)

Version: 1.0
Date: 2025-10-17

---

1. Introduction & Policy Statement

1.1. Commitment to AML/CFT Compliance

CONTEU Limited (the "Company") is fully committed to preventing the use of its services for money laundering, terrorism financing, proliferation financing, or any other illicit financial activity. This Anti-Money Laundering and Counter-Financing of Terrorism (AML/CFT) Policy Framework outlines the comprehensive measures, policies, and internal controls implemented to ensure rigorous compliance with the Financial Action Task Force (FATF) Recommendations, as well as the specific regulatory requirements imposed by the National Bank of Georgia (NBG) about Virtual Asset Service Providers (VASPs) operating within its jurisdiction.

The company recognizes the inherent risks associated with virtual assets (VAs) and is dedicated to proactively mitigating these risks through robust governance, technology, and human capital management. This framework is the foundation upon which all operational procedures relating to customer onboarding, transaction monitoring, and compliance reporting are built.

1.2. Scope and Applicability

This policy framework is mandatory and applies without exception to:

- All Directors and Executive Management.
- All permanent and temporary employees.
- All contractors, consultants, and agents acting on behalf of the company.

This scope governs all business lines and products involving the CONTEU token ecosystem, specifically encompassing:

- Initial Token Issuance and Distribution phases.
- The proprietary platform facilitates peer-to-peer (P2P) token transfers.
- On-ramping and off-ramping services interfacing with fiat currencies (where applicable).
- Interactions, settlements, and transfers involving third-party exchanges, custodians, and other VASPs.

1.3. Legal and Regulatory Basis

This framework is based on, and consistently reviewed against, the following core regulatory documents:

1. The FATF 40 Recommendations (as updated).
2. The specific NBG decrees governing VASPs in Georgia include licensing requirements and mandatory reporting obligations.
3. Relevant international sanctions regimes (UN, OFAC, EU).

---

2. Governance and Oversight

Effective AML/CFT compliance is overseen at the highest level and executed through designated officers.

2.1. AML Compliance Officer (AMLCO) Appointment and Authority

The Company shall appoint a dedicated, qualified, and sufficiently experienced Anti-Money Laundering Compliance Officer (AMLCO). This role must be independent of the operational business units to ensure impartiality in decision-making concerning high-risk matters.

Minimum Requirements for AMLCO:

- Demonstrated knowledge of international AML/CFT standards and local Georgian regulations.
- Sufficient seniority and direct reporting lines to the Board of Directors or equivalent governing body.
- Possession of adequate resources (budgetary and technological) to execute compliance duties.

Core Responsibilities of the AMLCO:

- **Program Management:** Developing, implementing, reviewing, and updating the comprehensive AML/CFT Program, including all supporting policies and procedure manuals.
- **Regulatory Interface:** Serving as the singular point of contact for regulatory bodies, including the NBG and the Financial Intelligence Unit (FIU).
- **Suspicion Oversight:** Reviewing, investigating, and approving the filing of all Suspicious Transaction Reports (STRs) or Suspicious Activity Reports (SARs).
- **Training:** Designing, scheduling, and documenting mandatory AML/CFT training for all relevant personnel, ensuring content reflects the latest regulatory guidance and emerging threats.
- **Reporting:** Preparing detailed, risk-calibrated quarterly compliance reports for the Board of Directors, detailing key metrics, compliance breaches, and necessary remediation actions.
- **VASP Due Diligence:** Overseeing the due diligence process for any third-party VASP partnerships.

---

3. Risk-Based Approach (RBA) Implementation

The company adopts a proactive Risk-Based Approach (RBA) as mandated by FATF Recommendation 1. Mitigation efforts must be commensurate with the identified risks.

3.1. Institutional Risk Assessment (IRA)

The Company will maintain a formal, documented Institutional Risk Assessment (IRA) conducted by the AMLCO, subject to Board review.

Frequency and Triggers:

- The IRA must be formally reviewed and updated at least **annually**.
- An extraordinary review must be triggered immediately upon any material change, including:

- Introduction of a new product or service feature (e.g., DeFi integration).
- Expansion into new geographic markets.
- Significant technological upgrades to the blockchain interaction protocol.
- Discovery of new, significant ML/TF typologies affecting the VASP sector.

3.2. Risk Factor Analysis

The IRA methodology will systematically evaluate inherent risks across four primary domains:

3.2.1. Customer Risk Profile

Assessment of the onboarding population:

- **PEPs:** Identification of domestic and foreign PEPs, their immediate family members (IFM), and close associates (CA).
- **High-Risk Jurisdictions:** Customers residing in or transacting heavily with jurisdictions identified by FATF, the IMF, or the NBG as having significant AML/CFT deficiencies.
- **Entity Structure Complexity:** Assessing the complexity of corporate structures (e.g., shell companies, bearer shares, and complex trust arrangements).

3.2.2. Geographic Risk Profile

Analysis of transaction origins and destinations:

- Exposure to regions known for high corruption perception indices (CPI).
- Jurisdictions subject to active international sanctions lists.
- Areas noted for a high incidence of cryptocurrency-related financial crime.

3.2.3. Product and Service Risk Profile

Evaluation of the CONTEU token and platform features:

- **Anonymity Features:** Assessment of any features that reduce traceability (e.g., high transaction limits, private transactions outside the main ledger).

- **Speed and Scale:** The potential for rapid, high-volume movement of funds across borders before manual intervention is possible.
- **Smart Contract Risk:** Risk associated with unverified or newly deployed smart contracts interacting with the token ecosystem.

3.2.4. Delivery Channel Risk Profile

Assessment of how services are accessed:

- Use of unverified or anonymous communication channels.
- Reliance on untested third-party integration points.

3.3. Risk Mitigation and Control Calibration

The controls applied must reduce the inherent risk to an acceptable residual risk level. This is achieved through risk-calibrated due diligence tiers:

Risk Level	Required Due Diligence Tier	Key Mitigation Actions
Low	Simplified Due Diligence (SDD)	Basic identity verification; reduced frequency of ongoing monitoring.
Medium	Standard Due Diligence (SDD)	Full CDD as per Section 4; automated transaction monitoring.
High	Enhanced Due Diligence (EDD)	Full CDD and source of wealth/funds verification; senior management approval; quarterly manual file review.

4. Customer Due Diligence (CDD) / Know Your Customer (KYC)

The company adheres strictly to FATF Recommendation 10 regarding the necessity of verifiable customer identification and ongoing monitoring.

4.1. Customer Identification Program (CIP)

No account opening or transaction processing exceeding the de minimis threshold (currently set at the equivalent of $500 USD/EUR) shall commence until the identity of the customer is verified.

4.1.1. Required Identification for Natural Persons:

1. **Full Legal Name:** As per official government-issued documentation.
2. **Date and Place of Birth:** Supporting documentary evidence required.
3. **Residential Address:** Official document dated within the last three months (e.g., utility bill, bank statement).
4. **Nationality and Citizenship.**
5. **Government-Issued Identification Number:** Unique identifier (e.g., passport number, national ID card number, driver's license number). A copy of the document must be retained.

4.1.2. Required Identification for Legal Entities (Corporations, Foundations, Trusts):

1. **Entity Legal Name and Registration Number:** As recorded by the appropriate corporate registry.
2. **Registered Address and Principal Place of Business.**
3. **Legal Status and Purpose of the Entity.**
4. **Identification of Beneficial Owners (BO):** Identification of all natural persons who directly or indirectly hold 25% or more of the equity interest or voting rights, or exercise equivalent control.
5. **Identification of Control Persons:** Identification of the natural persons authorized to act on behalf of the entity (e.g., directors, CEOs).
6. **Governing Documents:** Articles of Incorporation, Partnership Agreements, or Trust Deeds.

4.2. Customer Verification Procedures

Verification must be robust and independent. The company mandates a combination of document checks and liveness verification where feasible:

- **Document Authentication:** Use of recognized third-party database checks (e.g., World-Check, Dow Jones Risk & Compliance) and forensic document analysis tools to confirm the authenticity of submitted IDs.
- **Address Verification:** Use of utility bills, government correspondence, or credit reports. For remote onboarding, selfie video verification confirming that the person matches the ID document is required.
- **PEP Screening:** Ongoing screening against global PEP and sanctions databases at onboarding and periodic intervals.

4.3. Enhanced Due Diligence (EDD) Triggers

EDD procedures are mandatory when the risk assessment identifies the customer as high-risk.

4.3.1. Politically Exposed Persons (PEPs)

Establishing a relationship with a PEP requires:

- Approval from the AMLCO or a designated director *before* onboarding.
- Comprehensive documentation establishing the **Source of Wealth (SOW)**, how the individual accumulated their entire fortune, and the **Source of Funds (SOF)**, the origin of the specific funds entering the platform. This often requires audited financial statements or tax returns.
- A commitment to significantly more intensive ongoing monitoring, typically involving quarterly manual reviews of activity against expected profiles.

4.3.2. High-Risk Jurisdictions and Complex Structures

For entities or individuals connected to high-risk areas:

- Verification that the entity is genuinely operating within that jurisdiction (substance over form).
- Scrutiny of the correspondent banking or VASP relationships used by the entity.

- If the customer utilizes mixers or tumblers (which is highly discouraged), an immediate EDD review is triggered, potentially leading to account restriction.

4.4. Ongoing Monitoring and Profile Maintenance

Customer risk profiles are dynamic. Monitoring includes:

- **Transaction Profile Consistency:** Comparing transaction size, frequency, and counterparties against the established baseline documented during CDD.
- **Adverse Media Screening:** Automated and manual checks for negative news related to the customer or beneficial owners.
- **Data Refresh:** Requiring customers to re-verify core identity details (e.g., address proof) on a risk-based schedule (e.g., every 1–3 years).

---

5. FATF Recommendation 16: The "Travel Rule" Compliance

The company acknowledges the obligation to apply the FATF Travel Rule to virtual asset transfers, treating these transfers similarly to traditional wire transfers regarding data collection.

5.1. Policy on Originator/Beneficiary Information

The Company shall obtain, hold, and transmit required originator and beneficiary information for all CONTEU token transfers that exceed the applicable threshold (currently established by the NBG/FIU, generally USD/EUR 1,000).

5.2. Required Travel Rule Data Fields

For relevant transfers, the following minimum dataset must be captured and transmitted to the counterparty VASP:

Information Type	Originator (Sender)	Beneficiary (Receiver)
Name	Full Legal Name	Full Legal Name
Account/Wallet Identifier	Originating CONTEU Wallet Address	Receiving Wallet Address
Physical Address	Residential or Registered Address	Residential or Registered Address
Account Number	Originating Platform Account ID (if applicable)	Receiving Platform Account ID (if applicable)

Note: If the transaction is below the threshold, basic originator and beneficiary wallet addresses will be retained.

5.3. Technical Implementation of the Travel Rule

Given the decentralized nature of blockchain transactions, compliance necessitates secure technical solutions:

- **VASP Interoperability:** The company commits to integrating with established, FATF-compliant Travel Rule solutions (e.g., TRISA, Atomyze, or specialized integrations compliant with the NBG's preferred messaging protocols).
- **Data Security:** All transmitted PII (Personally Identifiable Information) must be encrypted using industry-standard protocols (e.g., PGP encryption) to ensure data confidentiality during transmission between VASPs.
- **Non-Cooperative Counterparties:** If a counterparty VASP cannot securely receive or validate the required Travel Rule information, the company reserves the right to:

- Block the transfer outright.
- Route the transfer through a compliant intermediary.
- Subject the transaction to immediate manual review by the AMLCO.

---

6. Suspicious Transaction Reporting (STR)

6.1. Identification of Suspicious Activity and Typologies

All employees are mandated to be vigilant for activities inconsistent with a customer's known profile or standard market behavior. The transaction monitoring system will employ heuristics and rule-based triggers, informed by the latest FATF typologies.

Common Red Flags Requiring Immediate Escalation:

- **Structuring (Smurfing):** Repeated transactions just below reporting thresholds designed to evade monitoring or reporting ($999 transactions followed by consolidation).
- **Velocity/Volume Mismatches:** Unusually large transfers immediately following account activation, or rapid movement of funds without a clear economic purpose.
- **Mixer/Tumbler Use:** Any direct or indirect interaction with known cryptocurrency mixing services, privacy coins, or anonymizing protocols.
- **Geographic Deviation:** Funds originating from or destined for wallets flagged as high-risk, sanctioned, or associated with cybercrime intelligence feeds.
- **Rapid Off-Ramping:** Large inflows of crypto funds that are almost immediately converted to fiat or withdrawn, especially without prior history.

6.2. Internal Reporting and Investigation Protocol

1. **Internal Triage:** Any employee suspecting activity must immediately cease non-essential interaction with the customer concerning the suspected activity and report findings via the designated confidential internal reporting channel to the AMLCO.

2. **AMLCO Investigation:** The AMLCO will conduct a timely, thorough investigation, gathering all relevant KYC documentation, transaction logs, IP data, and communication records.
3. **Decision Point:** Based on the investigation, the AMLCO will decide whether reasonable grounds for suspicion exist that the funds relate to ML/TF.
4. **Filing the STR:** If grounds exist, the AMLCO will prepare and submit an STR to the relevant Financial Intelligence Unit (FIU) in Georgia within the legally mandated timeframe (typically 24-72 hours of forming the suspicion).

6.3. Prohibition on Tipping Off

Strict internal controls are enforced to ensure that the customer, or any unauthorized employee, is **never informed** that an STR has been or will be filed. Violations of the tipping-off prohibition carry severe disciplinary action, up to and including termination and criminal referral.

---

7. Sanctions Compliance and Asset Freezing

The company operates under a zero-tolerance policy toward facilitating transactions involving sanctioned entities or individuals.

7.1. Screening Program

The company implements automated and periodic screening procedures against all relevant global sanctions lists:

- **Primary Lists:** United Nations Security Council Consolidated List, OFAC Specially Designated Nationals (SDN) List, and official EU Consolidated List.
- **Secondary Lists:** Relevant lists maintained by the NBG.

7.2. Screening Scope

Screening applies to:

- The primary account holder/legal entity.

- All identified Beneficial Owners (BOs).
- The originator and beneficiary wallet addresses involved in transfers above the monitoring threshold are cross-referenced with blockchain intelligence tools.

7.3. Action Upon Match

Any confirmed match (hard match) between a customer/transaction and a sanctions list will result in immediate, non-negotiable actions:

1. **Account Freeze:** Immediate suspension of all trading, withdrawal, or transfer capabilities related to the identified customer or asset.
2. **Internal Review:** Immediate review by the AMLCO and Legal Counsel to confirm the sanction applicability.
3. **Regulatory Notification:** Immediate reporting of the matched account/transaction to the relevant authorities as required by Georgian law, often involving asset freezing procedures pending official instruction.

---

8. Record-Keeping and Data Integrity

Compliance with FATF Recommendation 11 necessitates meticulous record-keeping to support the reconstruction of transactions and verification of compliance processes.

8.1. Retention Period

All records relating to the business relationship, CDD procedures, and transaction data shall be retained for a minimum period of **five (5) years** following the termination of the business relationship or the date of the transaction, whichever is later. This retention period aligns with the standard statutory requirements applicable to financial institutions in the primary jurisdiction.

8.2. Content of Records

The records maintained must be adequate to demonstrate compliance with all aspects of this framework:

- **Identity Records:** Copies of all KYC documents (IDs, corporate registries, proof of address).
- **Relationship Records:** Communications logs, relationship manager notes, and risk assessment scores throughout the customer lifecycle.
- **Transactional Records:** Comprehensive logs detailing the date, time, value (in CONTEU tokens and equivalent fiat), sender wallet, receiver wallet, and associated transaction hash for every on-chain or on-platform movement.
- **Compliance Activity Records:** All internal compliance reviews, Suspicious Activity Reports filed (along with related investigation files), and training attendance logs.

8.3. Data Integrity and Access

Records must be stored securely, ensuring integrity (immutability) and accessibility for regulatory inspection. Access to sensitive AML/CFT records is strictly controlled and limited only to the AMLCO, the Board, and authorized legal/audit personnel.

---

9. Training, Testing, and Remediation

Compliance effectiveness is maintained through continuous staff education and independent validation.

9.1. Comprehensive Training Program

The AMLCO shall administer a structured training program that evolves with the regulatory landscape and evolving ML/TF risks.

Training Requirements:

- **New Hires:** Mandatory AML/CFT induction training must be completed within 30 days of commencement of employment for all relevant personnel.
- **Annual Refresher:** All staff must undergo annual refresher training covering recent changes in FATF guidance, FIU directives, and specific typologies identified in the company’s latest IRA.

- **Role-Specific Modules:** Specialized training modules focusing on high-risk areas (e.g., EDD application for the onboarding team; Travel Rule protocol for the technical operations team).

9.2. Independent Testing and Audit

To ensure the AML/CFT framework is operating effectively, the company mandates periodic independent testing:

- **Frequency:** An independent internal or external audit of the entire AML/CFT program must be conducted at least every **two years**.
- **Scope:** The audit must test the adequacy of the risk assessment, the effectiveness of CDD implementation, the accuracy of transaction monitoring rules, and the handling of STRs.

9.3. Remediation and Policy Review

Findings from internal testing, regulatory examinations, or internal incidents must result in a formal remediation plan managed by the AMLCO. All material deficiencies identified must be tracked to resolution, with progress reported to the Board of Directors in the subsequent quarterly compliance report. This framework itself is subject to review concurrently with the IRA process.

---

10. Technology and Blockchain Analysis

The reliance on blockchain technology requires specialized analytical tools to maintain FATF compliance, particularly concerning the tracing of token movements.

10.1. Blockchain Tracing Tools

The Company shall contractually utilize advanced blockchain analytics software (e.g., Chainalysis, Elliptic, or equivalent providers approved by the NBG) to conduct forensic analysis:

- **Wallet Profiling:** Assigning risk scores to incoming and outgoing wallet addresses based on their historical activity (e.g., association with darknet markets, sanctioned exchanges, or mixers).

- **Tracing Flow:** Ability to trace the CONTEU token across multiple intermediary addresses to determine the true origin or final destination of funds, essential for STR substantiation.

10.2. Smart Contract Interaction Risk

All smart contracts interacting with the core CONTEU token mechanism must undergo a rigorous code audit before deployment. The audit must specifically assess for vulnerabilities that could be exploited for illicit gain, such as re-entrancy bugs or unauthorized minting capabilities that could disrupt AML controls.

10.3. Custody and Private Key Management

If the company assumes custodial functions over customer assets, the controls must meet stringent security standards equivalent to Tier-1 financial institutions, including multi-signature requirements, hardware security modules (HSMs), and geographical separation of key custodianship.

---

11. Glossary of Terms

Term	Definition
AML/CFT	Anti-Money Laundering / Counter-Financing of Terrorism.
AMLCO	Anti-Money Laundering Compliance Officer.
CDD	Customer Due Diligence.

EDD	Enhanced Due Diligence.
FIU	Financial Intelligence Unit (Georgia's authorized body).
FATF	Financial Action Task Force.
NBG	National Bank of Georgia.
PEP	Politically Exposed Person.
RBA	Risk-Based Approach.
STR	Suspicious Transaction Report.
VASP	Virtual Asset Service Provider.