REVEXIUM

Money Laundering and Terrorist Financing Prevention Policy

REVEXIUM

This **Money Laundering and Terrorist Financing Prevention Policy** (the "Policy") establishes the Company's framework for preventing, detecting, and mitigating financial crimes, including money laundering, terrorism financing, sanctions violations, fraud, corruption, and other predicate offenses in accordance with applicable AML/CTF legislation. All Clients and personnel engaging with the Company agree to adhere to this Policy as a condition of participation in the Company's services.

Article 1: LEGAL COMPLIANCE AND CORPORATE OVERSIGHT

1.1 The Company maintains a comprehensive compliance infrastructure designed to ensure full adherence to international and domestic AML and CTF regulations. This includes mandatory cooperation with regulatory authorities and law enforcement agencies upon reasonable suspicion of illicit activity.

1.2 Organizational governance requires dedicated compliance personnel, ongoing risk assessments, and routine audits to uphold operational integrity and prevent financial crime.

1.3 The Company adopts a strict zero-tolerance approach to financial crime, mandating that all employees and agents complete mandatory AML/CTF training and comply with monitoring and supervisory protocols.

1.4 Internal Reporting Lines: The Company establishes clear reporting lines for escalation of compliance concerns, ensuring whistleblowers can report suspected breaches without fear of retaliation.

Article 2: CLIENT VERIFICATION AND DUE DILIGENCE

2.1 Comprehensive identity verification is required for all prospective and existing Clients, including submission of legal, financial, and residency documentation as part of KYC procedures.

2.2 Clients must disclose the lawful source of funds for all transactions, with supporting documentation securely retained for auditing and regulatory purposes.

2.3 Third-party disclosure of client information is strictly limited to statutory requirements or regulatory obligations.

2.4 Clients authorize the Company to submit Suspicious Transaction Reports (STRs) and share relevant data with competent authorities in full compliance with legal obligations.

2.5 Verification standards are uniformly applied to all Clients, with no preferential treatment or exceptions permitted.

2.6 Politically Exposed Persons (PEPs): Enhanced due diligence applies to PEPs, their relatives, and close associates, including periodic reviews and heightened monitoring of account activity.

Article 3: RISK EVALUATION AND TRANSACTIONAL CONTROLS

3.1 The Company applies a risk-based approach to onboarding and ongoing monitoring, with high-risk Clients subjected to enhanced scrutiny.

3.2 Low-risk Clients may undergo simplified due diligence in accordance with regulatory guidance. Risk categorization is reviewed periodically and adjusted as needed.

3.3 Anonymous or fictitious entities are prohibited. Transactions executed on behalf of third parties require legally valid authorization documentation.

3.4 The Company reserves the right to reject, suspend, or terminate accounts or transactions that do not comply with documentation or compliance requirements.

3.5 Risk evaluations consider geographic factors, corporate structures, transactional patterns, and association with prohibited activities. Immediate account closure and reporting occur if connections to terrorist financing or illegal weapons are detected.

3.6 Automated Monitoring Tools: The Company may implement automated surveillance systems to detect unusual or suspicious patterns and generate alerts for compliance personnel.

Article 4: ONGOING MONITORING, RECORDS, AND ENFORCEMENT

4.1 Client transactions and account activities are monitored continuously against internal benchmarks, industry standards, and external watchlists.

4.2 Records related to due diligence, transactions, and compliance actions are securely maintained in accordance with legal retention periods and anonymized or destroyed after expiration.

4.3 Upon detection of suspicious activity, the Company may suspend accounts, restrict transactions, and report to regulatory authorities.

4.4 Employees must report any actual or suspected violations. Whistleblower protections are guaranteed under applicable law.

4.5 The Company may amend or update this Policy unilaterally. Updates will be communicated via official channels, and continued use constitutes acceptance.

4.6 Non-compliance with this Policy may result in account termination, legal reporting, or prosecution.

4.7 Escalation of High-Risk Transactions: Transactions identified as exceptionally high-risk must be escalated to senior compliance officers for approval or further investigation before execution.

Article 5: TRAINING, EDUCATION, AND AWARENESS

5.1 All personnel, including contractors and agents, are required to complete AML/CTF training upon onboarding and at regular intervals thereafter.

5.2 Training effectiveness is periodically evaluated to ensure personnel comprehension, compliance readiness, and adherence to internal procedures.

Article 6: POLICY REVIEW AND GOVERNANCE

6.1 The Company's AML/CTF framework is subject to regular internal audits, compliance reviews, and independent assessments to ensure effectiveness and regulatory alignment.

6.2 Audit findings, gaps, and deficiencies must be documented and addressed with corrective action plans, overseen by the Compliance or Risk Management function.

6.3 Continuous Improvement: The Policy shall be updated based on evolving regulatory requirements, operational risks, and lessons learned from internal reviews or industry developments.