Bronetix

Compliance Policy on Money Laundering and Terrorist Financing

Bronetix

This Compliance Policy on Money Laundering and Terrorist Financing (the **"Policy"**) defines the principles, controls, and governance mechanisms adopted by the Company to identify, deter, prevent, and respond to financial crime risks. These risks include, without limitation, money laundering, terrorist financing, sanctions evasion, fraud, bribery, corruption, and other related predicate offenses.

Adherence to this Policy is a mandatory condition for all Clients, employees, officers, contractors, and representatives who engage with the Company, its platforms, or its services.

Article 1: Regulatory Alignment and Compliance Governance

1.1. In fulfillment of its legal and ethical obligations, the Company operates a structured compliance framework designed to align with all applicable anti-money laundering and counter-terrorist financing laws, regulations, and supervisory expectations across relevant jurisdictions. This framework supports cooperation with competent authorities, regulators, and law enforcement bodies when legally required or when suspicious conduct is identified.

1.2. Oversight of financial crime prevention is embedded within the Company's governance architecture and includes the appointment of qualified compliance personnel, implementation of internal controls, periodic enterprise-wide risk assessments, and routine internal and external audits to validate effectiveness.

1.3. The Company enforces a strict intolerance for financial crime. All staff members, officers, and agents are required to comply with AML/CTF obligations, complete mandatory training programs, and adhere to internal surveillance, escalation, and reporting procedures as a condition of engagement.

1.4. Clear escalation pathways are maintained to ensure that suspected violations, irregularities, or compliance concerns may be reported promptly and confidentially. Individuals who report such concerns in good faith shall be protected against retaliation in accordance with applicable whistleblower protection laws.

Article 2: Client Identification, Verification, and Due Diligence Standards

2.1. Prior to establishing or maintaining any business relationship, the Company requires Clients to undergo comprehensive identification and verification procedures. These procedures include the submission and validation of identity documentation, residency information, and other data necessary to satisfy Know Your Customer requirements.

2.2. Clients are required to demonstrate the lawful origin of funds used in connection with the Company's services. Supporting documentation may be requested at onboarding and on an ongoing basis, and such records shall be securely retained in accordance with regulatory retention obligations.

2.3. Disclosure of Client information to external parties is strictly controlled and shall occur only where required by law, regulatory mandate, or competent authority request, and always in accordance with applicable data protection frameworks.

2.4. By engaging with the Company, Clients expressly authorize the submission of suspicious activity or transaction reports to relevant authorities and consent to the lawful exchange of information necessary to fulfill statutory AML/CTF obligations.

2.5. Client due diligence measures are applied consistently and objectively, without preferential treatment, exemptions, or waivers, regardless of account size, activity level, or relationship history.

2.6. Clients identified as Politically Exposed Persons, as well as their close associates and immediate family members, are subject to enhanced due diligence measures. These measures include heightened verification, ongoing monitoring, and periodic reassessment of risk exposure.

Article 3: Risk Assessment Methodology and Transaction Controls

3.1. The Company applies a risk-based methodology to Client onboarding, account maintenance, and transactional monitoring. Risk classifications are assigned based on objective criteria and inform the scope, intensity, and frequency of due diligence measures.

3.2. Where permitted by law, Clients assessed as presenting lower risk profiles may be subject to simplified due diligence procedures. Risk ratings are reviewed periodically and may be revised in response to changes in behavior, geography, or regulatory guidance.

3.3 The use of anonymous, fictitious, or nominee arrangements is strictly prohibited. Transactions conducted on behalf of third parties require valid legal authorization and are subject to enhanced verification and scrutiny.

3.4. The Company reserves the right to decline, suspend, restrict, or terminate accounts or transactions where documentation is incomplete, inconsistent, or non-compliant with AML/CTF requirements.

3.5. Risk evaluations incorporate factors such as geographic exposure, transactional behavior, ownership structures, industry risk, and association with restricted or prohibited activities. Where links to terrorist financing, weapons proliferation, or sanctioned entities are identified, immediate reporting and account action shall occur.

3.6. The Company may deploy automated monitoring and surveillance technologies to identify unusual, complex, or suspicious activity patterns. Alerts generated through such systems are reviewed by trained compliance personnel.

Article 4: Continuous Monitoring, Recordkeeping, and Enforcement Measures

4.1. Client accounts and transactions are subject to continuous monitoring against internal thresholds, regulatory indicators, and external sanctions or watchlists to detect potentially illicit activity.

4.2. Records relating to Client identification, transaction history, risk assessments, and compliance actions are maintained securely for legally mandated retention periods. Upon expiration, records are anonymized or destroyed in accordance with data protection requirements.

4.3. Where suspicious activity is detected, the Company may impose immediate restrictions, suspend access, or terminate accounts and shall submit reports to competent authorities as required by law.

4.4. All personnel are obligated to report known or suspected violations of this Policy. Reports made in good faith are protected under applicable whistleblower and employment laws.

4.5. The Company reserves the right to revise or update this Policy at its discretion. Amendments shall take effect upon publication through official channels, and continued engagement with the Company constitutes acceptance.

4.6. Failure to comply with this Policy may result in account closure, reporting to authorities, disciplinary action, or legal proceedings, depending on the severity of the breach.

4.7. Transactions assessed as presenting exceptional risk must be escalated to senior compliance management and may not be executed without documented approval following enhanced review.

Article 5: Training, Awareness, and Competency Development

5.1. All employees, officers, agents, and relevant third-party representatives are required to complete AML/CTF training upon commencement of engagement and at regular intervals thereafter to ensure continued competency.

5.2. Training programs are periodically reviewed and tested to assess effectiveness, comprehension, and alignment with evolving regulatory expectations and operational risk profiles.

Article 6: Oversight, Audit, and Continuous Enhancement

6.1. The Company's AML/CTF framework is subject to ongoing review through internal audits, compliance testing, and, where appropriate, independent assessments to verify effectiveness and regulatory conformity.

6.2. Identified deficiencies, audit findings, or control weaknesses must be formally documented and addressed through corrective action plans overseen by the Compliance or Risk Management function.

6.3. This Policy is maintained as a living framework and shall evolve in response to regulatory developments, emerging typologies, technological change, and lessons derived from internal or industry-wide events.