

AML Oversight and Compliance Standards

I. PURPOSE, SCOPE, AND REGULATORY COMMITMENT

I.I Policy Objective and Institutional Commitment

The Company operates within global financial markets and provides services involving the custody, transfer, and management of monetary assets. In recognition of the inherent risks associated with financial transactions, the Company has implemented comprehensive Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) compliance standards designed to prevent, detect, and report illicit financial activity.

This AML Oversight and Compliance Standards document establishes the internal controls, verification procedures, monitoring mechanisms, and reporting obligations adopted by the Company to safeguard its operations and uphold financial system integrity.

The Company maintains zero tolerance for activities involving:

- Money laundering
- Terrorist financing
- Tax evasion
- Fraud or financial misrepresentation
- Embezzlement
- Sanctions violations
- Any activity that may compromise regulatory compliance

II. LEGAL AND REGULATORY ALIGNMENT

II.I Adherence to Applicable AML Legislation

The Company conducts its operations in strict observance of applicable anti-money laundering laws, counter-terrorism financing regulations, sanctions regimes, and international financial compliance standards.

Where required, the Company cooperates fully with regulatory authorities, financial intelligence units, and law enforcement bodies in relation to suspicious transactions or ongoing investigations.

II.II Mandatory Reporting Obligations

Where suspicion arises that a transaction or Client behavior may be linked to unlawful activity, the Company may:

- File Suspicious Activity Reports (SARs) or equivalent regulatory disclosures
- Freeze or restrict account access
- Suspend or terminate services
- Withhold funds pending investigation
- Provide information to competent authorities

The Company is not obligated to inform the Client when such reporting is legally restricted.

III. CLIENT IDENTIFICATION AND VERIFICATION FRAMEWORK

III.I Mandatory Identity Verification

Prior to establishing a business relationship, each Client must undergo formal identity verification procedures under the Company's Know Your Customer (KYC) framework.

This includes, but is not limited to:

- Government-issued identification
- Proof of residential address
- Biometric verification where applicable
- Source of funds documentation
- Politically Exposed Person (PEP) screening
- Sanctions list screening

Failure to complete verification satisfactorily shall result in service denial.

III.II Source of Funds and Wealth Verification

Clients are required to provide transparent disclosure concerning the origin of funds intended for deposit or trading. Supporting documentation may include:

- Bank statements
- Tax filings
- Salary certificates
- Business ownership documents
- Inheritance records
- Investment portfolio statements

The Company reserves the right to reject funds where legitimate origin cannot be reasonably established.

IV. RISK-BASED DUE DILIGENCE FRAMEWORK

IV.I Risk Categorization Model

Clients are classified under a risk-based assessment model that evaluates:

- Geographic exposure
- Business activity
- Transaction behavior
- Political exposure
- Industry risk
- Payment methods used
- Volume and frequency of transactions

IV.II Enhanced Due Diligence (EDD)

Where heightened risk indicators are present, the Company applies Enhanced Due Diligence measures, including:

- Ongoing transaction monitoring
- Additional identity verification
- Senior management approval

- Increased reporting oversight
- Periodic compliance reviews

IV.III Simplified Due Diligence

Low-risk Clients may be subject to streamlined verification processes consistent with applicable regulations.

V. THIRD-PARTY REPRESENTATION CONTROLS

V.I Authorized Representatives

The Company establishes business relationships only with properly identified individuals or legally registered entities.

Where a third party acts on behalf of a Client, formal authorization documentation must be submitted and approved.

V.II Prohibition of Unauthorized Transactions

Transactions initiated by unauthorized third parties may be rejected, reversed, or invalidated without notice.

VI. ONGOING MONITORING AND RECORD KEEPING

VI.I Continuous Transaction Surveillance

The Company maintains automated and manual monitoring systems to detect:

- Structuring or smurfing behavior
- Rapid fund movement patterns
- Circular trading schemes
- Abnormal trading volume
- Inconsistent transaction activity
- Suspicious jurisdiction transfers

VI.II Record Retention

Transaction records, identity documents, communication logs, and risk assessments are retained in accordance with regulatory retention requirements.

Access to such records may be restricted to preserve confidentiality and legal compliance.

VII. INTERNAL GOVERNANCE AND AUDIT CONTROLS

VII.I Employee Training and Awareness

The Company conducts ongoing AML training programs for employees to ensure:

- Awareness of evolving financial crime risks
- Proper identification of suspicious activities
- Understanding of internal reporting procedures
- Compliance with regulatory obligations

VII.II Internal Audit and Compliance Review

Regular internal audits are conducted to assess:

- Policy effectiveness
- System integrity
- Risk exposure
- Procedural compliance

Corrective measures are implemented where deficiencies are identified.

VIII. CLIENT OBLIGATIONS AND COOPERATION

VIII.I Duty to Cooperate

Clients must fully cooperate with any compliance inquiry, including providing requested documentation within specified timelines.

Failure to cooperate may result in:

- Temporary account suspension
- Permanent account termination
- Fund restrictions
- Reporting to regulatory authorities

VIII.II Accurate Information Requirement

Clients must ensure that all submitted information remains accurate, current, and complete. Misrepresentation may constitute a material breach of the Service Terms.

IX. REFUSAL OR TERMINATION OF RELATIONSHIP

IX.I Right to Decline Transactions

The Company may decline, reverse, or suspend any transaction that:

- Lacks a legitimate commercial purpose
- Cannot be verified
- Raises compliance concerns
- Involves sanctioned jurisdictions
- Is inconsistent with Client risk profile

IX.II Termination Authority

Where AML risks cannot be satisfactorily mitigated, the Company reserves the right to terminate the business relationship without prior notice, subject to applicable legal requirements.

X. CONTINUOUS POLICY REVIEW

The Company reserves the right to update or amend these AML Oversight and Compliance Standards in response to regulatory developments or evolving financial crime risks.

Continued use of the Company's services constitutes acceptance of such amendments.