NUXEROS

AML AND CTF COMPLIANCE POLICY

Last Updated: April 14, 2026

1. REGULATORY FRAMEWORK AND POLICY OBJECTIVES

1.1 Purpose and Scope

This AML and CTF Compliance Policy *(the "Policy")* establishes the standards, controls, and procedures implemented by the Company to prevent, detect, and mitigate risks associated with financial crime.

This includes, but is not limited to, money laundering, terrorist financing, fraud, tax evasion, corruption, and other unlawful financial activities that may compromise the integrity of the Company's operations.

1.2 Commitment to Legal and Regulatory Compliance

The Company operates in accordance with applicable international standards and domestic regulatory requirements relating to anti-money laundering and counter-terrorism financing.

The Company reserves the right to cooperate fully with regulatory bodies, law enforcement agencies, and governmental authorities in connection with any investigation involving suspected unlawful financial conduct.

1.3 Zero-Tolerance Policy

The Company adopts a strict zero-tolerance approach toward any form of financial crime.

Any activity that is reasonably suspected to involve illicit financial conduct shall result in immediate action, which may include account restriction, termination of services, and reporting to relevant authorities.

1.4 Governance and Internal Oversight

The Company shall maintain an internal compliance structure responsible for implementing, monitoring, and enforcing this Policy.

Such structure may include designated compliance personnel, reporting mechanisms, and internal review processes to ensure adherence to AML and CTF obligations.

2. CLIENT IDENTIFICATION AND DUE DILIGENCE REQUIREMENTS

2.1 Identity Verification *(KYC Obligations)*

The Company shall implement robust client identification procedures designed to verify the identity of all Clients prior to granting access to its services.

Clients are required to provide accurate, complete, and current information, and must promptly update any changes to their personal or financial details.

2.1.1 Documentation Requirements

Clients may be required to submit documentation including, but not limited to:

- Government-issued identification;
- Proof of residential address;
- Financial documentation demonstrating source of funds;
- Additional documentation as deemed necessary by the Company.

2.1.2 Ongoing Verification

The Company reserves the right to conduct periodic re-verification of Client information to ensure continued compliance with regulatory requirements.

2.2 Source of Funds and Wealth Verification

Clients must demonstrate that all funds deposited or transacted through the Company originate from legitimate and lawful sources.

The Company may request supporting documentation at any time to substantiate such declarations.

2.3 Authorization for Data Collection and Disclosure

By engaging with the Company, the Client expressly consents to the collection, storage, processing, and, where required, disclosure of personal and financial data to authorized entities for compliance purposes.

This includes, but is not limited to, the filing of Suspicious Transaction Reports (STRs) or equivalent regulatory disclosures.

2.4 Uniform Application of Due Diligence Standards

All Clients are subject to the same verification standards, regardless of status, relationship, or affiliation.

No exemptions shall be granted where such exemption may compromise compliance obligations.

2.5 Legal Capacity and Eligibility Assessment

The Company reserves the right to evaluate the legal capacity of any Client to engage in financial transactions.

Where a Client is determined to lack sufficient legal or financial capacity, the Company may restrict or terminate access to its services.

3. RISK ASSESSMENT AND TRANSACTION MONITORING

3.1 Risk-Based Approach

The Company applies a risk-based methodology to assess and categorize Clients according to their level of exposure to financial crime risks.

This assessment shall consider factors including jurisdiction, transaction behavior, source of funds, and business profile.

3.2 Enhanced Due Diligence *(EDD)*

Clients identified as higher risk, including politically exposed persons *(PEPs)*, individuals from high-risk jurisdictions, or those exhibiting unusual transaction patterns, shall be subject to enhanced due diligence procedures.

Such procedures may include additional documentation, ongoing monitoring, and increased scrutiny.

3.3 Simplified Due Diligence *(SDD)*

Where permitted by applicable regulations, simplified due diligence measures may be applied to lower-risk Clients, provided that such measures remain compliant with AML and CTF standards.

3.4 Prohibition of Anonymous and Third-Party Accounts

The Company strictly prohibits the use of anonymous, fictitious, or unverifiable identities.

Where a third party acts on behalf of a Client, appropriate legal authorization, such as a valid power of attorney, must be provided and approved.

3.5 Right to Refuse or Terminate Relationships

The Company reserves the right to decline, suspend, or terminate any Client relationship or transaction where required documentation is not provided or where risk thresholds are exceeded.

3.6 Transaction Monitoring and Surveillance

The Company shall continuously monitor transactions and account activity to identify suspicious patterns, anomalies, or behaviors indicative of financial crime.

Monitoring systems may include automated tools, manual reviews, and risk-based alerts.

3.7 Prohibited Activities and High-Risk Indicators

The Company shall take immediate action in cases involving activities linked to:

- Terrorism financing;
- Proliferation of weapons;
- Organized criminal activity;
- Fraudulent or deceptive financial conduct.

4. RECORDKEEPING, REPORTING, AND ENFORCEMENT MEASURES

4.1 Ongoing Monitoring and Data Analysis

Client activity shall be subject to continuous monitoring and evaluation against internal controls, regulatory standards, and international watchlists.

4.2 Record Retention Obligations

All Client records, including identification documents and transaction histories, shall be retained for a period consistent with applicable legal and regulatory requirements.

Such records may be archived, anonymized, or securely disposed of upon expiration of retention periods.

4.3 Reporting of Suspicious Activity

Where suspicious activity is identified, the Company shall take appropriate action, including:

- Filing regulatory reports;
- Restricting or freezing accounts;
- Terminating services;
- Cooperating with authorities.

4.4 Internal Reporting and Whistleblower Protection

Employees and representatives are required to report any suspected breaches of this Policy.

The Company shall ensure that such reports are handled confidentially and that individuals are protected from retaliation.

4.5 Enforcement Actions

Failure by Clients to comply with this Policy may result in:

- Account suspension or closure;
- Restriction or recovery of funds where permitted by law;
- Reporting to regulatory or law enforcement authorities;
- Legal proceedings where applicable.

4.6 Policy Updates and Amendments

The Company reserves the right to amend this Policy at any time.

Updates shall take effect upon publication through official communication channels, and continued use of the Company's services shall constitute acceptance.

4.7 Cross-Border Compliance Considerations

Clients acknowledge that AML and CTF requirements may vary across jurisdictions.

The Company reserves the right to apply stricter compliance measures where necessary to meet international regulatory standards.