

FINANCIAL CRIME PREVENTION POLICY

(Incorporated by Reference into and Forming an Integral Part of the Usage Terms and Policies)

1. Scope, Purpose, and Regulatory Commitment

1.1 Policy Objective

For the purpose of maintaining a secure, transparent, and compliant operating environment, this Policy establishes the framework through which the Company identifies, prevents, detects, and reports activities associated with financial crime, including but not limited to money laundering, terrorist financing, fraud, corruption, tax evasion, and other illicit financial conduct.

By accessing or utilizing the Company's services, you expressly acknowledge and agree that all activities conducted through your account shall be subject to continuous monitoring, verification, and regulatory scrutiny in accordance with this Policy and all applicable laws.

1.2 Regulatory Alignment

The Company operates in strict adherence to applicable international standards, including but not limited to anti-money laundering (AML) and counter-terrorism financing (CTF) regulations, and shall implement internal controls designed to ensure compliance with:

- (a)** Applicable financial crime prevention laws in relevant jurisdictions;
- (b)** Regulatory obligations imposed by competent authorities;
- (c)** International best practices, including risk-based compliance frameworks;
- (d)** Internal governance, monitoring, and reporting protocols.

1.3 Zero-Tolerance Principle

Under no circumstances shall the Company knowingly facilitate, participate in, or tolerate any activity that may be directly or indirectly associated with financial crime. Any suspicion or confirmation of such conduct shall result in immediate enforcement action, including account restriction, reporting to authorities, and potential legal proceedings.

2. Client Identification and Verification (KYC Framework)

2.1 Mandatory Verification Requirements

Prior to granting access to any services, the Company shall undertake comprehensive identity verification procedures. You are required to submit accurate, complete, and verifiable documentation to establish:

- (a) Your legal identity;
- (b) Your residential address;
- (c) Your financial profile and economic background;
- (d) The lawful origin of your funds.

Failure to satisfy these requirements may result in the denial, suspension, or termination of your account.

2.2 Ongoing Verification Obligations

Client verification is not a one-time process. The Company reserves the right to request updated documentation at any stage of the business relationship, particularly where:

- (a) Transaction patterns change materially;
- (b) Risk classification is elevated;
- (c) Regulatory obligations require updated due diligence;
- (d) Suspicious activity indicators are identified.

3. Source of Funds and Wealth Assessment

3.1 Disclosure Requirements

As a condition of using the Company's services, you must provide sufficient evidence demonstrating that all funds deposited or transacted originate from lawful sources.

This may include, but is not limited to:

- (a) Employment or business income records;
- (b) Bank statements;
- (c) Investment portfolios;
- (d) Tax declarations or financial disclosures.

3.2 Verification and Risk Assessment

The Company reserves the right to independently assess the legitimacy of your financial background. Where inconsistencies, irregularities, or unexplained sources of funds are identified, enhanced due diligence measures shall be applied.

4. Transaction Monitoring and Reporting Obligations

4.1 Continuous Monitoring

All account activity shall be subject to automated and manual monitoring systems designed to detect:

- (a) Unusual transaction patterns;
- (b) High-frequency or high-value transactions inconsistent with profile;
- (c) Structuring or layering activities;
- (d) Indicators of fraud, manipulation, or illicit conduct.

4.2 Suspicious Activity Reporting

Where suspicious activity is identified, the Company shall:

- (a) Conduct internal investigations;
- (b) Restrict or suspend account activity where necessary;
- (c) File reports with relevant authorities without prior notice to the Client;
- (d) Retain all relevant records for regulatory purposes.

You acknowledge that such reporting obligations may be carried out without disclosure to you.

5. Risk-Based Due Diligence Framework

5.1 Risk Classification

Clients shall be categorized based on risk exposure, taking into account:

- (a) Geographic location;
- (b) Nature of financial activity;
- (c) Source of funds;
- (d) Transaction behavior;
- (e) Political exposure or public position.

5.2 Enhanced Due Diligence (EDD)

For high-risk Clients, the Company may implement additional measures, including:

- (a) Requesting supplementary documentation;
- (b) Conducting enhanced monitoring;
- (c) Limiting account functionality;
- (d) Requiring periodic re-verification.

6. Politically Exposed Persons (PEPs) and High-Risk Jurisdictions

6.1 Identification of PEPs

Where a Client is identified as a Politically Exposed Person (PEP), or is associated with one, the Company shall apply heightened scrutiny.

6.2 Jurisdictional Risk

Clients residing in or transacting through jurisdictions identified as high-risk or non-compliant with AML standards may be subject to:

- (a) Additional verification requirements;
- (b) Transaction limitations;
- (c) Refusal of services where appropriate.

7. Third-Party Transactions and Authorization Controls

7.1 Prohibition of Anonymous Activity

The Company strictly prohibits anonymous accounts or transactions conducted without verified identity.

7.2 Authorized Third Parties



Where a third party is authorized to act on your behalf:

- (a) A valid Power of Attorney must be submitted;
- (b) Full verification of the third party is required;
- (c) The Company retains full discretion to reject or revoke such authorization.

8. Refusal, Suspension, and Termination Rights

8.1 Grounds for Action

The Company may refuse, suspend, or terminate any account or transaction where:

- (a) Required documentation is not provided;
- (b) Information is false, misleading, or incomplete;
- (c) Suspicious activity is detected;
- (d) Regulatory obligations necessitate such action.

8.2 Immediate Enforcement

Such actions may be implemented without prior notice where deemed necessary to protect regulatory compliance or operational integrity.

9. Record Keeping and Data Retention

9.1 Retention Obligations

The Company shall retain all relevant records, including identification data and transaction history, for the period required under applicable laws.

9.2 Regulatory Access

Such records may be disclosed to regulatory authorities, auditors, or law enforcement agencies as required.

10. Internal Controls and Compliance Oversight

10.1 Independent Monitoring

The Company maintains internal audit and compliance functions responsible for:

- (a) Reviewing adherence to AML/CTF policies;
- (b) Conducting periodic risk assessments;
- (c) Ensuring operational compliance with regulatory standards.

10.2 Non-Discrimination in Enforcement

All Clients shall be subject to the same compliance standards, regardless of relationship status, referral source, or account size.

11. Client Legal Capacity and Eligibility

11.1 Assessment of Capacity

The Company reserves the right to evaluate whether a Client possesses the legal capacity to enter into and maintain a business relationship.

11.2 Immediate Action

Where legal incapacity is identified, the Company may suspend or terminate the account without liability.

12. Ongoing Monitoring and Compliance Review

12.1 Continuous Assessment

Client profiles and transaction activities shall be periodically reviewed to ensure continued compliance.

12.2 Regulatory Updates

The Company may update its procedures to align with evolving legal and regulatory requirements without prior notice.

13. Client Responsibilities and Cooperation

13.1 Duty to Cooperate

You agree to fully cooperate with all compliance requests, including the submission of documentation and clarification of transactions.

13.2 Consequences of Non-Compliance

Failure to comply may result in:

- (a) Account restrictions;
- (b) Suspension of services;
- (c) Reporting to authorities;
- (d) Termination of the business relationship.

14. Policy Amendments and Enforcement

14.1 Right to Amend

The Company reserves the right to modify this Policy at any time to reflect regulatory developments or operational requirements.

14.2 Binding Effect

Continued use of the Company's services constitutes acceptance of any updated provisions.