AML and KYC Policy

SECTION 1. INTRODUCTION AND APPLICABILITY

1.1 Purpose and Scope

1.1.1 This **AML and KYC Policy** supplements and forms part of the Service Usage Policy governing your access to and use of the Company's Platform and Services.

1.1.2 The Company is committed to maintaining effective measures designed to prevent, detect, deter, and report activities associated with money laundering, terrorist financing, sanctions violations, fraud, corruption, tax evasion, financial crime, and other unlawful conduct.

1.1.3 This Policy establishes the standards, procedures, and controls implemented by the Company to comply with applicable anti-money laundering, counter-terrorist financing, customer identification, and financial crime prevention requirements.

1.1.4 The Company adopts a risk-based approach to customer verification, transaction monitoring, and ongoing compliance oversight.

1.1.5 By accessing or using the Services, opening an Account, or conducting transactions through the Platform, you acknowledge and agree to comply with the requirements set forth in this Policy.

1.2 Compliance Commitment

1.2.1 The Company maintains policies, procedures, controls, and monitoring systems designed to support compliance with applicable legal and regulatory obligations relating to financial crime prevention.

1.2.2 The Company reserves the right to implement additional compliance measures where deemed necessary to address emerging risks, regulatory developments, or operational requirements.

SECTION 2. CUSTOMER IDENTIFICATION AND VERIFICATION

2.1 Know Your Customer Requirements

2.1.1 The Company requires all Users to complete identity verification procedures before access to certain Services may be granted.

2.1.2 Verification measures are intended to confirm the identity of Users, assess risk exposure, and support compliance with applicable legal and regulatory obligations.

2.1.3 Users may be required to provide information including:

(a) full legal name;

(b) date of birth;

(c) nationality;

(d) residential address;

(e) contact information; and

(f) any additional information reasonably requested by the Company.

2.2 Verification Documentation

2.2.1 The Company may require submission of documents including:

(a) government-issued identification;

(b) proof of residential address;

(c) proof of identity verification photographs or biometric verification;

(d) source of funds documentation; and

(e) other supporting materials necessary for verification purposes.

2.2.2 The Company reserves the right to request updated documentation at any time.

2.3 Customer Identification Program

2.3.1 The Company maintains procedures designed to verify the identity of each User prior to establishing or continuing a business relationship.

2.3.2 The Company may use internal reviews, electronic verification tools, independent databases, third-party service providers, and other lawful verification methods.

SECTION 3. CUSTOMER DUE DILIGENCE

3.1 Risk-Based Assessment

3.1.1 The Company applies a risk-based approach when assessing Users and business relationships.

3.1.2 Risk assessments may consider factors including:

(a) geographical location;

(b) occupation or business activities;

(c) transaction patterns;

(d) source of funds;

(e) source of wealth;

(f) account activity; and

(g) other relevant risk indicators.

3.2 Standard Due Diligence

3.2.1 The Company may conduct customer due diligence procedures to understand the nature and purpose of the business relationship.

3.2.2 Users may be required to provide information sufficient to establish the legitimacy of their intended use of the Services.

3.3 Enhanced Due Diligence

3.3.1 Enhanced Due Diligence measures may be applied where a User presents elevated financial crime risk.

3.3.2 Enhanced Due Diligence may include:

(a) additional identity verification;

(b) source of wealth verification;

(c) senior management review;

(d) enhanced transaction monitoring; and

(e) periodic compliance reviews.

SECTION 4. SOURCE OF FUNDS AND TRANSACTION MONITORING

4.1 Source of Funds Requirements

4.1.1 Users may be required to provide information demonstrating the legitimate origin of funds deposited or used through the Platform.

4.1.2 Acceptable documentation may include bank statements, employment records, business documentation, investment records, tax records, or other evidence reasonably requested by the Company.

4.2 Source of Wealth Verification

4.2.1 In higher-risk situations, the Company may require information regarding the broader origin of a User's accumulated assets or wealth.

4.3 Transaction Monitoring

4.3.1 The Company maintains systems and procedures designed to monitor account activity and transactions for indicators of suspicious behavior.

4.3.2 Monitoring activities may include review of transaction volumes, transaction frequency, payment methods, account activity patterns, and other risk indicators.

SECTION 5. SANCTIONS SCREENING AND HIGH-RISK RELATIONSHIPS

5.1 Sanctions Compliance

5.1.1 The Company may conduct sanctions screening against applicable governmental, regulatory, and international sanctions lists.

5.1.2 The Company reserves the right to refuse, restrict, suspend, or terminate Services where sanctions-related concerns are identified.

5.2 Politically Exposed Persons

5.2.1 The Company may identify and assess Users who qualify as Politically Exposed Persons *(PEPs),* family members of PEPs, or close associates of PEPs.

5.2.2 Additional due diligence measures may be applied where appropriate.

5.3 High-Risk Jurisdictions

5.3.1 The Company may apply enhanced controls to Users associated with jurisdictions presenting elevated money laundering, terrorist financing, sanctions, corruption, or financial crime risks.

SECTION 6. SUSPICIOUS ACTIVITY AND REGULATORY REPORTING

6.1 Suspicious Activity Detection

6.1.1 The Company maintains procedures designed to identify unusual, suspicious, or potentially unlawful activity.

6.1.2 Indicators may include unusual transaction patterns, inconsistent account activity, unverifiable information, attempts to circumvent controls, or other risk indicators.

6.2 Reporting Obligations

6.2.1 Where required by law, the Company may report suspicious activity to relevant regulatory authorities, law enforcement agencies, financial intelligence units, or other competent authorities.

6.2.2 Users acknowledge that the Company may be prohibited from disclosing the existence of certain investigations, reviews, or reports.

SECTION 7. THIRD-PARTY REPRESENTATION AND ACCOUNT CONTROLS

7.1 Authorized Representatives

7.1.1 The Company may permit authorized third parties to act on behalf of a User where appropriate authorization documentation has been provided and approved.

7.1.2 The Company reserves the right to reject any authorization that cannot be satisfactorily verified.

7.2 Account Restrictions

7.2.1 The Company may restrict, suspend, freeze, reject, delay, or terminate transactions, Accounts, or Services where:

(a) verification requirements are not satisfied;

(b) requested information is not provided;

(c) suspicious activity is detected;

(d) legal or regulatory concerns arise; or

(e) compliance risks cannot be adequately managed.

SECTION 8. RECORDKEEPING, MONITORING, AND COMPLIANCE OVERSIGHT

8.1 Record Retention

8.1.1 The Company may retain records relating to identity verification, transactions, compliance reviews, investigations, monitoring activities, and communications for legal, regulatory, audit, operational, and compliance purposes.

8.2 Ongoing Monitoring

8.2.1 User information, risk profiles, and account activity may be periodically reviewed and updated throughout the duration of the business relationship.

8.2.2 Users may be required to provide updated information or documentation during periodic reviews.

8.3 Internal Audits and Compliance Reviews

8.3.1 The Company may conduct audits, compliance assessments, monitoring activities, and internal reviews to evaluate the effectiveness of its AML and KYC framework.

SECTION 9. EMPLOYEE TRAINING AND REGULATORY COOPERATION

9.1 Employee Training

9.1.1 The Company may provide ongoing training and awareness programs to employees, officers, contractors, and representatives regarding AML, KYC, sanctions compliance, fraud prevention, and financial crime risks.

9.2 Regulatory Cooperation

9.2.1 The Company cooperates with competent authorities, regulators, law enforcement agencies, and other authorized bodies as required by applicable law.

9.2.2 Information may be disclosed where required to satisfy legal or regulatory obligations.

SECTION 10. USER RESPONSIBILITIES AND POLICY ADMINISTRATION

10.1 User Cooperation

10.1.1 Users must cooperate fully and promptly with requests for information, documentation, verification, clarification, or compliance reviews.

10.1.2 Failure to cooperate may result in delays, restrictions, suspension, termination of Services, or other actions deemed appropriate by the Company.

10.2 Policy Amendments

10.2.1 The Company reserves the right to amend, revise, supplement, replace, or update this Policy at any time.

10.2.2 Amendments shall become effective upon publication through the Platform or other communication channels designated by the Company.

10.3 User Acknowledgement

10.3.1 By accessing or using the Services, opening an Account, or conducting transactions through the Platform, you acknowledge that you have read and understood this AML and KYC Policy.

10.3.2 You agree to comply with the requirements, procedures, and controls established under this Policy.