KYC/AML Policy

Last updated: June 12, 2025

1. INTRODUCTION

This Know Your Customer (KYC) and Anti-Money Laundering (AML) Policy is designed to ensure compliance with applicable laws and international best practices in preventing the use of our platform for money laundering, terrorist financing, and other illegal activities. This policy applies globally and is designed to accommodate country-specific compliance requirements.

2. CUSTOMER DUE DILIGENCE (CDD)

We conduct customer due diligence on all users, including:

- Identification and verification of individuals and legal entities;
- Collection of full name, date of birth, nationality, address, and identification documents;
- Enhanced due diligence (EDD) for high-risk individuals or jurisdictions.

3. VERIFICATION PROCEDURES

Verification may include but is not limited to:

- Government-issued ID (passport, national ID, or driver's license);
- Proof of address (utility bill, bank statement);
- Biometric verification and facial recognition, where applicable.

4. ONGOING MONITORING

We monitor user transactions to detect suspicious behavior, including:

- Unusual transaction volumes;
- Activity inconsistent with profile;
- Transactions involving high-risk jurisdictions or sanctioned individuals.

5. SANCTIONS AND PEP SCREENING

We screen customers against global sanctions lists and databases of politically exposed persons (PEPs), such as:

- UN, EU, OFAC, FATF lists;
- Other government and regulatory watchlists.

6. RECORD KEEPING

All KYC records and transaction histories are retained for a minimum of 5 years or longer if required by local regulations.

7. REPORTING

We report suspicious activity to the relevant authorities where legally obligated and cooperate fully with law enforcement and regulatory bodies.

8. RISK-BASED APPROACH

We apply a risk-based approach (RBA) to assess and mitigate financial crime risks, adjusting procedures based on client risk profiles and regulatory requirements.

9. EMPLOYEE TRAINING

Employees involved in compliance functions receive regular training in KYC/AML procedures and evolving global standards.

10. PRIVACY AND DATA PROTECTION

All personal data is collected and processed in accordance with applicable data protection laws such as the GDPR, CCPA, and others where applicable.

11. VERIFICATION ON DEMAND

The Company reserves the right to require identity verification or additional due diligence measures from any user at any time, regardless of whether such verification has previously been completed. This may include, but is not limited to, cases of suspicious activity, changes in account behavior, regulatory updates, internal compliance reviews, or random audits. Failure to comply with a verification request may result in account restrictions, suspension, or termination of services.

12. REVIEW AND UPDATES

This policy is reviewed periodically and updated to reflect changes in legislation, regulations, or internal processes.