

KNOW YOUR CUSTOMER POLICY

The Company applies a comprehensive Know Your Customer (KYC) policy as part of its broader compliance obligations. This policy is aimed at ensuring the lawful use of our platform, the prevention of fraud, identity misuse, money laundering, and the financing of terrorism, in accordance with applicable legal and regulatory standards.

1. Purpose of KYC Measures

KYC procedures are implemented to:

- Verify the identity of each Customer;
- Ensure that all funds used within the platform originate from lawful sources;
- Prevent the platform from being used for criminal or fraudulent purposes;
- Comply with relevant anti-money laundering (AML), counter-terrorism financing (CTF), and regulatory obligations.

2. Initial Identity Verification

The Company conducts identity verification during the registration process and prior to permitting certain account activities. At minimum, each Customer is required to provide:

- Full legal name;
- Date of birth;
- Permanent residential address.

Depending on the nature, frequency, or size of transactions, the Company reserves the right to request additional information and supporting documentation in Company's sole discretion.

Furthermore, certain transactions may be subject to enhanced due diligence procedures to ensure compliance with applicable regulations.

All documents submitted must be clear, valid, unaltered, and verifiable. In case of doubt, the Company may request notarised documents or conduct further checks, including biometric verification or database screening.

3. Triggers for Additional Verification

Enhanced verification measures may be applied in the following cases:

- Cumulative deposits, withdrawals or transactions reaching or exceeding the applicable threshold;
- Detection of unusual or inconsistent account activity;
- Residence in or transactions involving high-risk jurisdictions;
- Indications of identity fraud, impersonation, or use of third-party payment methods;
- Classification as a Politically Exposed Person (PEP) or connection to a sanctioned entity.

In such cases, the Company may request documentation confirming the source of funds or wealth, additional identity documents, transaction history, or banking information. All data may be subjected to real-time screening tools and risk profiling.

4. Ongoing Due Diligence and Monitoring

KYC is not a one-time requirement. The Company implements continuous monitoring of Customer activity, including:

- Regular updates to Customer information;
- Transactional behavior analysis;
- Re-verification upon significant changes (e.g., change of address, payment method, or jurisdiction);
- Application of enhanced due diligence for high-risk accounts or behaviors.

Where necessary, the Company reserves the right to suspend or restrict account functions pending completion of additional due diligence procedures.

5. Refusal to Comply

If the Customer fails or refuses to provide requested information or documentation, the Company may take the following measures:

- Suspend or restrict account access;
- Freeze deposits, withdrawals, or gameplay;
- Terminate the account relationship;
- Report the case to the appropriate regulatory or investigative authorities.

The Company shall not be liable for any losses or delays resulting from such action where it is necessary for compliance with its regulatory obligations or the protection of the platform.

6. Fraud and Internal Review

Where fraudulent activity, misrepresentation, or the use of falsified documents is suspected, the Company may:

- Block or permanently close the Customer's account;
- Cancel pending payments and transactions;
- Launch an internal investigation and involve competent external authorities;
- Retain or forfeit funds where permitted under applicable law or regulation.

Any such actions will be proportionate, documented, and based on objective findings. The Company will take all reasonable steps to ensure confidentiality and legal compliance during such processes.

7. Document Validity and Security

All documents submitted to the Company are handled in accordance with applicable data protection laws. The Company applies appropriate security measures to store and process KYC data and retains such records for the legally required period following account closure or final transaction.