

Anti-Money Laundering (AML) and Know Your Customer (KYC Policy)



These Terms and Conditions ("Terms") govern the use of services provided by **Orbit Option Ltd** ("Company," "we," "our," or "us"). By opening an account, accessing, or using our platform or services, you confirm your agreement to be legally bound by these Terms.

1. OBJECTIVE

This Anti-Money Laundering (AML) and Know Your Customer (KYC) Policy ("Policy") establishes the principles and procedures adopted by **Orbit Option Ltd** to prevent the misuse of its services for money laundering, terrorist financing, or any form of illicit financial activity.

The Company and its affiliates are firmly committed to:

- Ensuring full compliance with applicable international AML laws and standards;
- Detecting and preventing transactions related to illicit financial activities;
- Preserving the integrity of its operations and protecting clients and stakeholders.

2. DEFINITIONS

For the purposes of this Policy, the following definitions apply:

Money Laundering:

The process of concealing the origins of illegally obtained money, typically through transfers involving financial institutions or legitimate businesses. It generally involves three stages: placement, layering, and integration.

Terrorist Financing:

The provision or collection of funds, by any means, directly or indirectly, with the intention or knowledge that such funds will be used, in whole or in part, to carry out terrorist acts.

Client:

Any natural or legal person utilizing the Company's services for trading, investment, or any form of financial transaction.

3. AML / KYC REQUIREMENTS

The Company implements and enforces the following mandatory AML and KYC procedures:

3.1 Client Identification (KYC)

- All clients must provide valid, government-issued identification documents (e.g., passport, national ID card, or driver's license).

- Failure to comply within five (5) business days from account registration may result in immediate suspension of access to the platform and services.

3.2 Verification of Source of Funds

- Clients must present clear and verifiable evidence of the origin of deposited funds (e.g., recent bank statements, payslips, contracts, or business documentation).
- Deposits deemed unverifiable may result in cancellation of trades and retention of any profits generated from such funds, pending investigation.

3.3 Transaction Monitoring

- All transactions are subject to ongoing monitoring and surveillance to detect irregular or suspicious patterns.
- Transactions inconsistent with a client's risk profile, or involving sanctioned or high-risk jurisdictions, may be blocked.
- The account may be suspended pending further investigation.

3.4 Prohibition of Third-Party Use

- Use of client accounts by unauthorized third parties is strictly prohibited.
- If a deposit is made by a third party into a client's account:
 - The account will be immediately blocked;
 - The funds will be returned to the original sender;
 - The account will be permanently suspended after verification procedures are completed.
- Account reactivation will not be permitted, except in exceptional circumstances with formal justification and express approval from the Compliance Department.
- The client may be reported to relevant authorities if there is any indication of an attempt to conceal the origin of funds or other suspicious behavior.

4. NON-COMPLIANCE AND SANCTIONS

Where clear evidence or reasonable suspicion of money laundering or terrorist financing exists, the Company shall:

- Freeze and block the client's account immediately;
- Cancel all active or pending trades;
- Retain and withhold any profits or gains derived from suspicious activity;
- Report the incident to competent authorities without prior notice to the client;
- Fully cooperate with local and international enforcement agencies.

5. EMPLOYEE RESPONSIBILITIES

5.1 Training and Capacity Building

- All employees shall undergo mandatory training in Anti-Money Laundering (AML), Know Your Customer (KYC), and Compliance at the time of onboarding.
- Training must be renewed annually or whenever there are material changes in regulations or internal procedures.
- Employees involved in client onboarding, financial transactions, or risk management must participate in specialized and advanced compliance training modules as determined by the Compliance Department.

5.2 Obligation to Report

- Employees must report any suspicious transaction or behavior to the designated Compliance Officer or AML team without delay.

Failure to report suspicious activity may result in disciplinary action.

6. REGULATORY COMPLIANCE FRAMEWORK

Orbit Option Ltd aligns its AML and KYC procedures with globally recognized standards and best practices, including but not limited to:

- Client Due Diligence (CDD) and Enhanced Due Diligence (EDD);
- Risk-Based Approach (RBA) for categorizing client risk levels;
- Screening against global watchlists, sanctions lists, and Politically Exposed Persons (PEPs) databases;

- Reporting of Suspicious Transactions (STRs) to competent authorities;
- Secure storage and confidentiality of client information in compliance with applicable data protection laws;
- Use of video calls and digital tools for remote identity verification;
- Verification through official government-issued identification and supporting documentation;
- Implementation of the Financial Action Task Force (FATF) Forty Recommendations;
- Compliance with relevant anti-money laundering provisions under the USA PATRIOT Act (2001), where applicable;
- Observation of applicable local AML legislation.

7. POLICY ENFORCEMENT

Senior management shall maintain and oversee a robust internal compliance program, with designated personnel responsible for implementing and supervising this Policy across all departments and business units.

Violations of this Policy by clients, employees, or third parties may result in:

- Disciplinary action, including termination of service agreements or employment;
- Reporting to law enforcement or regulatory authorities;
- Legal action where appropriate.

8. REVIEW AND AMENDMENT

This Policy shall be reviewed periodically, at least once per calendar year, and updated as necessary to reflect changes in:

- Legal or regulatory requirements;
- Business operations;
- Industry standards and regulatory expectations.

Amendments shall become effective upon publication on the Company's official platform or website.