

1. General Provisions

Verastox (hereinafter referred to as the “Company”) is committed to maintaining high standards in the field of anti-money laundering (AML) and countering the financing of terrorism (CFT).

The Company takes the necessary measures to ensure that Clients, Investors, Agents, Intermediaries and other parties involved in the business are not involved in various forms of illegal activity, including, but not limited to: money laundering, terrorist financing, proliferation of weapons of mass destruction, purchase and sale of narcotic drugs, blackmail, smuggling, concealment of corruption schemes, tax evasion and cybercrime.

This Policy provides general information to prospective or existing Clients of the Company and sets out the Company’s general obligations regarding Client verification and the measures taken to detect and prevent money laundering and terrorist financing.

Before registering a trading account on the platform, the Client confirms that they have read and agreed to the Company’s Anti-Money Laundering Policy and the List of Prohibited Jurisdictions.

2. What is meant by “Anti-Money Laundering (AML)”

Anti-Money Laundering (AML) is a set of measures, procedures and legislative acts aimed at detecting and preventing attempts to convert illegally obtained funds into legitimate assets.

Concealing the source of funds from financial regulators or law-enforcement authorities constitutes a financial crime and entails serious consequences.

One result of the rapid development of the financial industry has been the adoption of legal acts and laws aimed at combating money laundering. These internationally recognized measures have made it more difficult for companies and individuals involved in illegal activities to evade regulatory and law-enforcement authorities.

3. Anti-Money Laundering and Counter-Terrorist Financing Policy adopted by Verastox

The Company fully complies with the laws, statutes and regulations of the Cook Islands aimed at combating money laundering and terrorist financing. Detailed information on these laws and regulations can be found on the website of the Financial Supervisory Service (FSC) of the Cook Islands.

Money laundering and terrorist financing are criminal offenses under the applicable laws of the Cook Islands.

In accordance with the Financial Transactions Act 2017 (FIRA), the Company has developed the following Anti-Money Laundering and Counter-Terrorist Financing Program (hereinafter referred to as the "AML Program").

3.1 Establishment of the Anti-Money Laundering Department (AML/Compliance Department)

The Anti-Money Laundering Department oversees compliance with Verastox's AML Program.

The Anti-Money Laundering Department is responsible for:

- Developing, implementing and updating the internal anti-money laundering policy in compliance with FIRA.
- Training Company employees to identify suspicious financial transactions.
- Assisting the Financial Intelligence Service in detecting and preventing suspicious financial activity.
- Informing the Board of Directors and senior management of the Company about compliance with the AML Program and financial risks.
- Screening and monitoring the Company's Clients.

The Anti-Money Laundering Department is headed by a senior AML specialist (MLRO) appointed by the Board of Directors.

3.2 Mandatory "Know Your Customer" (KYC) Policy

The "Know Your Customer" policy (hereinafter, KYC) is a mandatory procedure for verifying the Client's identity. It helps protect the interests of Clients and the Company by minimizing the risk of unlawful activity.

Under applicable law, financial institutions are prohibited from opening anonymous trading accounts.

The KYC procedure includes, but is not limited to, verification of the following Client information:

- Authenticity of documents.
- Authenticity of personal data.
- Email address and telephone number.
- Country of residence.

The Company reserves the right to request additional information to complete the KYC procedure where necessary. Submission of incomplete

or inaccurate information by the Client may result in refusal or termination of services.

Client verification is carried out by submitting documents electronically through a third-party service provider.

Confidential information collected by the Company may be provided to a third party only where the request for such information has been made in accordance with applicable law.

Questions related to the KYC procedure should be sent to info@ladsora-group.com.

3.3 Automated Risk Assessment System

The Company uses an automated risk assessment system to identify unreliable Clients and high-risk transactions.

The Company reserves the right to configure and modify the risk assessment system as necessary.

The Anti-Money Laundering Department regularly monitors Clients flagged by the risk assessment system.

For security purposes, the Company does not provide public access to information about the risk assessment system or the Company's internal procedures.

Based on data analysis, the Anti-Money Laundering Department assesses risks and takes the necessary measures.

3.4 Informing Company Employees about the Anti-Money Laundering Policy

The Anti-Money Laundering Policy (AML policy) applies not only to wrongdoers attempting to legitimize illegally obtained funds, but also to employees of financial institutions who participate in monitoring and processing transactions.

The Anti-Money Laundering Department regularly informs Company employees about AML guidelines and conducts training aimed at identifying suspicious patterns used by organizations and individuals to launder money.

If, when processing transactions, a Company employee suspects misconduct based on AML guidelines and this Policy, the employee forwards the information to the head of the department and the Anti-Money Laundering Department for further review.

3.5 Provisions on Politically Exposed Persons (PEP)

The term “Politically Exposed Person” (Politically exposed person, PEP) in the context of this Policy is defined in accordance with section 3 of the Financial Transactions Act (FIRA) and includes:

- An individual who performs an important public function within a country or at the international level.
- Family members and associates of such individual, as defined by the Financial Transactions Act (FIRA).

A Client who has the status of a Politically Exposed Person (PEP) must provide the Anti-Money Laundering Department with copies of documents confirming such status.

Copies of the documents must be sent by email to info@ladsora-group.com before registering a trading account on the platform.

Each case of establishing a business relationship with Politically Exposed Persons (PEP) is discussed privately between the interested parties in accordance with applicable law.

Under applicable law, the Company is required to obtain information about Politically Exposed Persons (PEP) using its services. The Company reserves the right to use third-party services to confirm Politically Exposed Person (PEP) status and to request additional information where necessary.

3.6 Provision on Sanctioned Persons (Sanctioned Persons)

Verastox does not provide services to sanctioned persons.

For the purposes of this Policy, a “sanctioned person” means any individual or legal entity included in any sanctions-related list of specially designated persons, including, but not limited to:

- U.S. OFAC Consolidated Sanctions List (non-SDN);
- U.S. OFAC Specially Designated Nationals and Blocked Persons List (SDN);
- INTERPOL notices;
- EU Consolidated List of Persons Subject to Financial Sanctions;
- Israeli lists of terrorist organizations and unauthorized associations;
- United Nations Security Council Consolidated List;
- Other lists of sanctioned persons.

Prospective Clients included on a sanctions list are prohibited from registering trading accounts on the platform.

Clients whose sanctions status has been updated resulting in their inclusion on any sanctions list must immediately report this by email to info@verastox.com

The Company reserves the right to use third-party services to identify and confirm the sanctions status of Clients and may request additional information if it deems this necessary.

4. Storage of Personal Data

The Company reserves the right to store and process personal data obtained during Client identification, verification and financial transactions, including, but not limited to:

- Information provided by the Client for identity verification.
- Methods used to deposit and withdraw funds.
- Information about the Client obtained from publicly available databases.
- Any discrepancies arising during the Client identity verification process.

The Company retains personal data in English for six years from the date of the last financial activity in the Client's personal account or the closure of the account. The Company also retains information about suspicious Client activity for six years.