



## AML Policy

### What is AML?

Anti-money laundering (AML) is a term mainly used in the financial and legal industries to describe the legal controls that require financial institutions and other regulated entities to prevent, detect, and report money laundering activities. Anti-money laundering (AML) refers to a set of procedures, laws and regulations designed to stop the practice of generating income through illegal actions.

The AML Policy of the Company undertakes all reasonable and appropriate procedures related to money laundering prevention, financing of terrorism, and other illegal activities. The Company has prepared AML Policy to ensure the highest possible voluntary compliance under national and international AML standards and it will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls.

In order to help the government fight the funding of terrorism and money laundering activities and apart of our AML Compliance Program, we are required to obtain and record information and documentation that help confirm the Client's identity or provide additional information regarding the Client. This information may be requested at account opening or during periodic reviews conducted on existing Clients.

The Company's AML Policy includes:

- Compliance Officer;
- Internal control;
- Customer due diligence;
- Maintaining records;

### Compliance Officer

The duties of the Compliance Officer include:

- Monitoring the Company's compliance with AML obligations;
- Monitoring and control the Client's trading activity;
- Monitoring the Client's deposits and withdrawals;
- Overseeing communication and employee training;

The Compliance Officer also ensures that the Company keeps and maintains all the required AML records and will ensure that suspicious activity reports are provided to the proper law enforcement.



## Internal control

This AML Policy has been duly approved by the Board of Directors to oversee compliance with applicable AML Laws and Standards.

The Company undertakes the Client's risk assessment based on:

- Sufficiency and adequacy of identification documents submitted by the Client;
- Client's trading activity;
- Manner and other information about funds deposit and withdrawal;
- Guidance notes circulated by various governmental and intergovernmental organizations;

The Company may internally categorize the Client as a low-risk, medium-risk, or a high-risk user on the basis of the aforementioned assessment. In order to maintain the integrity of the risk assessment process, the results of the Client's risk assessment will not be disclosed to the Client.

## Customer due diligence

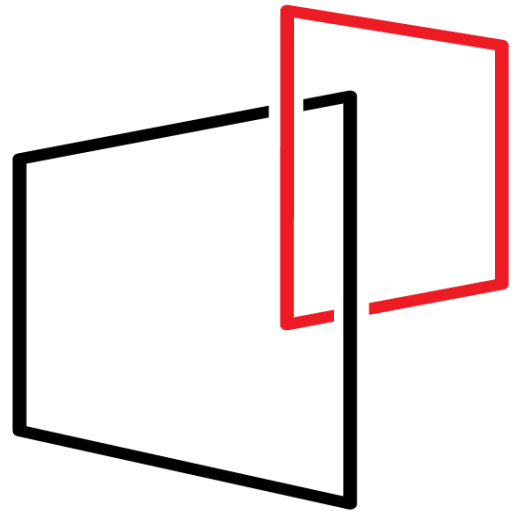
One of the international standards for preventing illegal activity is customer due diligence ("CDD"). According to CDD, the Company establishes its own verification procedures within the standards of anti-money laundering frameworks.

The Company may collect the following information<sup>1</sup> according to CDD:

- Individual Clients.  
Name; date of birth; email address; phone number and residential address; photograph; copies or certified copy of any Valid Documents;
- Business Clients.  
Business name; name, contact details, photograph, and copy of Valid Documents of the authorized representative, one certified copy of one of incorporation/registration Certificate (as the case may be); memorandum and articles of association/partnership deed (as the case may be); board resolution/other authorization documents giving authority to the representative chosen to execute transactions on the website;

In addition to the above, the Company can reserve the right to verify the Client's identity through non-documentary means or both. The Company may also use non-documentary means if there are some uncertain about the true identity of the Client. The Company may use the following non-documentary methods to verify identity:

- Confirming email validity;
- Confirming telephone number validity;
- Confirming the Client's location using, among others, the Client's IP address;



All of which may be carried out by an automated or manual process.

If the Company believes any information obtained from the Client hereunder is:

- Inadequate or incomplete;
- False or misleading;
- Insufficient resulting in an inability to readily verify the same;
- Appearing on any Sanctions Lists;

The Company may in sole discretion either refuse or terminate (as the case may be) the registration of such account or require such Client to verify the Valid Documents submitted by him again. The Company may also, in sole discretion, refuse to open any new trading accounts, terminate existing Client's account after giving due notice, or refuse to process any transactions on the Website if the Company is unable to verify any information due to non-cooperation of the Client, or if such transactions are likely to have an material adverse effect on the Company for being in violation of any applicable laws or industry best-practice guidelines.

*<sup>1</sup> Personal data is be processed in a manner that ensures appropriate security of the personal data, including protection from unauthorized or unlawful processing and from accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').*

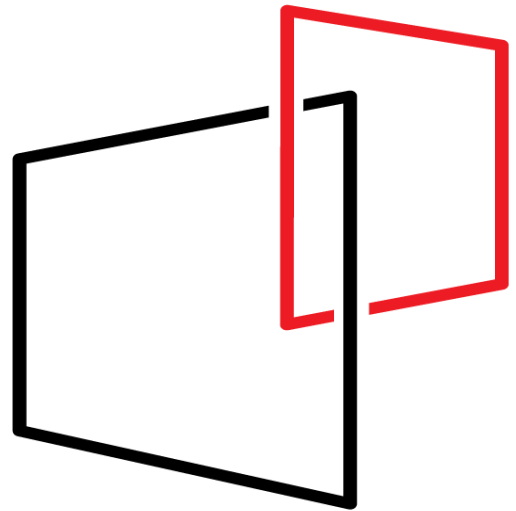
## **Monitoring and control activities**

The purpose of monitoring and control activities is to protect the Company from risks and to monitor and control on a permanent basis whether the Company's operations are carried out in accordance with national and international AML standards. Monitoring and control activities are executed by the Compliance Officer.

Monitoring and control activities include:

- Monitoring and control of Clients and transactions in the high risk group;
- Monitoring and control of complex and extraordinary transactions;
- Controlling, through the sampling method, whether the transactions do not exceed a predetermined limit consistent with the Client's risk-profile;
- Monitoring all transactions, through both manual screening and use of software-based algorithms, in order to promptly identify and highlight any suspicious activity;
- Controlling, completing and updating the information and documents about the Client;

Also the Company may regularly monitor, through both manual screening and using software-based algorithms, all transactions, in order to promptly identify and highlight any suspicious activity and the Company may cancel all transactions where was identified any suspicious (fraud) activity.



On detection of any suspicious (fraud) activity, the Company reserves the right to take appropriate actions without any prior notification to the Client, which includes, without limitation:

- Refusing to open any new trading accounts;
- Blocking existing Client's trading accounts and close open trading orders;
- Restricting and/or blocking further access to the website;
- Cancelling all deposit/withdrawal transactions where was identified any suspicious (fraud) activity;
- Notifying the appropriate enforcement authorities regarding the suspicious activities of any Client;

## **Maintaining records**

Under applicable AML Laws and Standards, the Company is required to maintain and preserve the following information and/or data:

- Records of all transactions executed by the Client, for a period of at least 5 (Five) years from the date of each;
- Records of all suspicious transactions, whether executed or attempted, for a period of at least 10 (Ten) years, including but not limited to the information about the date of remittance;
- Identification records of Clients (including but not limited to the Valid Documents submitted pursuant to the clause titled 'Customer Due Diligence' above), during the subsistence of and for a period of at least 5 (Five) years from the date of termination of such Client;