

# AML Policy

## 1. Scope of the policy

This Policy is to prohibit and actively pursue the prevention of money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. The Company requires its officers, employees to adhere to these standards in preventing the use of its products and services for money laundering purposes.

For the purposes of this Policy, money laundering is the participation in any transaction that seeks to conceal or disguise the nature or the origin of funds derived from the illegal activities. Money laundering involves not only the proceeds of drugs trafficking, but funds related to other illegal activities, including fraud, corruption, organized crime, terrorism and many other crimes. Generally the money laundering consists of three stages:

- Placement: introduction of cash originating from illegal / criminal activities into financial or non-financial institutions.
- Layering: separating the proceeds of criminal activities from their source through the use of layers of complex financial transactions. These layers are designed to hamper the audit trail, disguise the origin of funds and provide anonymity.
- Integration: placing the laundered proceeds back into the economy in such a way that they re-enter the financial system as apparently legitimate funds.

Terrorist financing is described as techniques, similar to those used by money launderers, where funds are provided for terrorist activity by individuals who wish to conceal the ultimate beneficiaries and the sponsors of the funds. It involves both funds raised from legitimate sources as well as criminal sources.

This Policy is developed and periodically updated by the Money Laundering Compliance Officer of the Company based on the general principles set up by the Board of Directors of the Company in relation to the prevention of money laundering and terrorist financing.

The Policy applies to all employees of the Company and aims to setup key roles and responsibilities for the staff members as well as to ensure compliance with the following legislation:

- THE PREVENTION AND SUPPRESSION OF MONEY LAUNDERING AND TERRORIST FINANCING LAWS No. 188(I)/2007 of 2007-2019 (the Law)
- DIRECTIVE (EU) 2015/849 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing
- DIRECTIVE OF THE CYPRUS SECURITIES AND EXCHANGE COMMISSION FOR THE PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING (the AML Directive)
- Any other Directives, Circulars and Guidelines issued by the Cyprus Securities and Exchange Commission (CySEC), the Unit of Combating Money Laundering

(MOKAS) and any other authority entrusted with the task of combating Money Laundering.

The Company has established principles and procedures to prevent money laundering and combat terrorism financing, in accordance with the risk profile of its products, services, clients and geographic locations.

Each employee of the Company, whose duties are associated with the provision of products and services of the Company and who directly or indirectly deals with the clientele of the Company, is expected to know the requirements of the applicable laws and regulations which affect his or her job responsibilities, and it shall be the affirmative duty of such employee to carry out these responsibilities at all times in a manner that complies with the requirements of the relevant laws and regulations

All amendments and/or changes of the current version of the Policy must be approved by the Company's Board of Directors.

## **2. Clients' acceptance policy**

Inadequate understanding of the client's profile and purpose of investment activity may expose the Company to a number of risks. In order to minimize such risks, the Company has developed the Client Acceptance Policy.

## **3. Risk-based approach**

The Company applies appropriate measures and procedures, on a risk based approach, so as to focus its effort in those areas where the risk of money laundering and terrorist financing appears to be higher. This approach will enable the Company to assign to its clients the following risk categories:

- High risk clients
- Medium risk clients
- Low risk categories

## **4. Dynamic Risk Management**

Risk Management is a continuous process, carried out on a dynamic basis. Risk assessment is not an isolated event of a limited duration. Client's activities change as well as the services and financial instruments provided by the Company change. The same happens to the financial instruments and the transactions used for money laundering or terrorist financing.

## **5. Know Your Client Procedures**

The prime method for preventing money laundering is by carrying out "Know Your Client" procedures. With thorough knowledge of clients, counterparties and the origin of client's funds, unusual or suspicious behaviour can be identified, including false identities, unusual transactions, changing behaviour or other indicators where laundering may be occurring.

The Company ensures that the clients' identification records remain completely updated with all relevant identification data and information throughout the business relationship. The Company examines and checks, on a regular basis, the validity and adequacy of the clients' identification data and information it maintains, especially those concerning high risk clients.

## 6. Reporting of Suspicious Transactions

Suspicious transactions are transactions or other activities that have no apparent lawful purpose or is not the sort in which a particular client would normally be expected to engage in, and the Company knows of no reasonable explanation for the transaction or activity after examining the available facts, including the background and possible purpose of the transaction or activity. The Company, in cases where there is an attempt of executing transactions which knows or suspects that are related to money laundering or terrorist financing, reports, through the MLCO its suspicion to MOKAS.

## 7. Record Keeping

The Company must maintain records of:

- All the documents and information which are necessary to comply with the customer due diligence requirements
- The supporting evidence and records of transactions, which are necessary to identify transactions, including the name and address (or identification code) of counterparties.
- Any additional documents/information obtained during the relationship
- All checks and reports obtained from open sources and third-parties in respect of the client, as well as all results for the screening on sanctions' lists, PEP and other watchlists

Details of all relevant business transactions carried out for clients for a period of seven years after the end of the business relationship with their customer or after the date of an occasional transaction.

This information may be used as evidence in any subsequent investigation by the authorities. The records kept provide audit trail evidence during any subsequent investigation. In practice, the business units of the Company will be routinely making records of work carried out for clients in the course of normal business and these records should be archived.