APPROVED

by the decision of the Board

*of UAB **„Digital Virgo Payment"***

dated 27th, February 2020 No. 1

UAB „DIGITAL VIRGO PAYMENT" ANTI-MONEY LAUNDERING/COMBATING THE FINANCING TERRORISM AND SANCTIONS POLICY

I. Purpose and Objective

The purpose of this Policy is to set the high-level principles and standards of management of financial crime risks, including money laundering, terrorist financing and sanctions breaches, for **UAB „Digital Virgo Payment"** (hereinafter referred to as **Institution**). The objective of this policy is to ensure regulatory compliance and to establish an internal framework that minimizes the risk of sanctions breaches and abuse Institution's products and services for money laundering and terrorist financing purposes.

The Institution shall carry out its business aiming to ensure effective prevention of money laundering and terrorism financing (hereinafter referred to as ML/TF) as required by Law on the prevention of money laundering and terrorist financing of Lithuania.

Taking this into account, all employees of the Institution shall adhere to the procedures of and requirements for the implementation of the ML/TF prevention measures as outlined herein.

II. Scope and application

The Policy applies to all employees and persons, all functions, all units in the Institution. The aim of the Instituton is not only to comply with relevant legal requirements, but also to mitigate and reduce the potential risk to the Institution of our clients using our products, services and delivery channels to launder the proceeds of illegal activity, fund terrorist activity or perform transactions in breach of financial sanctions.

III. Requirements

The Institution, in order to protect its reputation and meet its legal and regulatory obligations, is committed to design and implement a cost effective system to minimize the risks of the Institution being used by potential money launderers or designated terrorists. In implementing this Policy Institution shall adopt a risk-based approach as per the applicable regulatory requirements.

The following Acts cover the current legal frame for the Institution's anti-money laundering and financial sanctions regime:

- Law on the prevention of money laundering and terrorist financing of Lithuania;

- Implementing procedures approved by Bank of Lithuania and Lithuanian Financial Crime Investigation Service under the Ministry of the Interior of Republic of Lithuania;

- Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (hereinafter referred to as EU AMLD V);

- Applicable sanctions regimes.

IV. Terms

Money laundering and terrorist financing (AML/CTF) for the purpose of this Policy, the act of Money Laundering shall have the same meaning as provided in Article 1(3) of the AMLD IV (EU)(2015/849) amended by EU AMLD V (EU) (2018/843), which provides that it, when committed intentionally, encompasses; - (a) the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action; - (b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity; - (c) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity; - (d) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in points (a), (b) and (c).

Money laundering shall be regarded as such even where the activities which generated the property to be laundered were carried out in the territory of another Member State or in that of a third country."

The act of terrorist financing for the purpose of this Policy shall have the same meaning as provided in Article 1(5) of the EU AMLD IV (2015/849) amended by EU AMLD V (EU) (2018/843), which provides that it encompasses "the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 1 to 4 of Council Framework Decision 2002/475/JHA". For the purpose of this Policy the act of Terrorist financing refers to the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, in order to carry out an act of terror, or that the funds will be used to support any terrorist group, persons or association.

Financial sanctions are measures imposed by Lithuania and/or other national governments of market areas where Institution carries activities and multinational bodies which seek to alter the behaviour and decisions of other national governments or non-state actors that may (i) threaten the security of the global community, or (ii) violate international norms of behaviour (e.g. human rights violations).

The Institution must comply with the following sanctions measures:

1. The United Nations (UN) Security Council consolidated sanctions list;

2. The EU's consolidated list of persons, groups and entities;

3. The US Department of the Treasury, Office of Foreign Assets Control (OFAC) sanctions lists:

4. The US Department of the Treasury, Financial Crimes Enforcement Network (FinCEN) list;

Risk based approach (RBA). The Institution shall apply a risk based approach (hereinafter - RBA) to AML/CTF. The RBA encompasses identifying, assessing and understanding the ML/TF risks to which the Institution is exposed and to take measures proportionate to those risks for the purpose of mitigating them effectively. This means that the range, degree, frequency or intensity of controls will be more comprehensive in situations assessed as posing a higher ML/TF risk while these measures will be reduced in situations assessed as posing a lower ML/TF risk. Applying a RBA, thereby, allows the Institution to target its resources in the most efficient manner.

Financial crime. For the purpose of this Policy, Financial crime is used as the collective term for ML/TF and violations of Financial Sanctions.

V. The principles

The Institution cooperates with natural persons and legal entities:

- that are residents and non-residents of Lithuania;
- whom the Institution may identify in accordance with client identification terms;
- the origin of whose funds and wealth is known to the Institution;
- whose activity and the origin of whose funds and wealth is legal and may not harm the Institution's reputation;
- whose beneficial owners (of legal entities) are known to the Institution;
- who are ready to cooperate with the institution providing and updating the required information on a regular basis.

The Institution shall not start cooperating/provide service for anonymous, fictitious persons or under a false name.

The Institution shall obtain proof to identify legal and/or beneficial owners of all service users/clients and shall implement a remediation program to ensure that client due diligence rules have been complied with for legacy customers by reviewing the entire client relationship and regularly updating client information to comply with additional information requirements prescribed by legal acts.

The Institution performs an on-going due diligence to monitor transactions/activities of customers for anti money laundering and related purposes.

The Institution is undertaking a number of initiatives to strengthen its ability to ensure its compliance with the requirements outlined in this Policy. The Institution shall, therefore, continually assess its existing policies, procedures, controls and IT system and make necessary changes so as to be most effective in accordance with the risk based approach.

V. GOVERNANCE, DISTRIBUTUON OF ROLES AND RESPONSIBILITIES

Through this Policy, the Board of Institution ensures that there is a robust approach within the Institution to prevent money laundering, terrorist financing and breaches of financial sanctions. It is the responsibility of the Board to ensure that the Institution complies with the measures set in this Policy. The Head of Legal, Compliance and Risk Management is Board member who is responsible for implementing this Policy. He is Institution's Money Laundering Reporting Officer (hereinafter - MLRO)) with the responsibility to ensure that the Institution complies with the legal requirements and whose duties shall include the monitoring day-to- day implementation of the measures and procedures adopted under this Policy and cooperation with Lithuanian Financial Crime Investigation Service.

Before being appointed MLRO, Institution assesses the candidate's competence, work experience and qualifications. In evaluating of competence, experience and qualifications must take into account the level and nature of the individual's education, professional development, the nature and duration of the professional work experience, other factors that may affect the individual's competence, experience and qualifications, risk management knowledge relating to the implementation of measures to prevent money laundering and terrorist financing.

The central role of the MLRO is to act as a contact point to whom a report is to be made by the staff of any information or other matter which gives rise to a knowledge or suspicion that client is engaged in money laundering or the funding of terrorism. After receiving a report, it rests with the MLRO to decide whether the report gives rise to knowledge or suspicion that client is engaged in money laundering or the funding of terrorism.

Other responsibilities of MLRO include:

- monitoring of the day-to-day execution of the Institution’s AML CFT program and procedures;
- assessment of the new products and services of the Institution in the scope of possible money laundering risks;
- comprehensive implementation of international sanctions prevention in the Institution;
- cooperation with the Regulator (Bank of Lithuania) in the sphere of AML CFT, regulatory and statistical reporting;
- anually reporting to the Board of the Inxstitution about the AML CFT program performing;
- ensuring all employees are periodically informed of any changes in AML CFT legislation, policies, and procedures, as well as current developments and changes in money laundering or terrorist activity financing schemes;
- training the Employees in the AML CFT sphere;
- anually assessment of the level of exposure to the money laundering and terrorist financing risk in the Institution;
- ensuring adaptation of the Institution’s internal procedures and processes in the event of changes to the AML CFT regulations;
- prepare all necessary amendments to the AML CFT program in line with the risk assessment results;
- conducting fraud investigation cases, cooperation with law enforcement institutions.

The MLRO may not assign the responsibility provided for under the internal AML CFT procedures and in statutory law to another person, and any transfer by him of the rights, obligations, and responsibility may be done only to persons approved by Director of the Institution and shall require a decision of the Director (CEO).

The Board

The Board is responsible for the overall Compliance policy of the Institution and ensuring adequate resources are provided for the proper training of staff and the implementing of risk systems. This includes computer software to assist in oversight. The Board will receive and consider annual compliance reports sent by the MLRO.

Director (CEO). Three lines of defence

The Director (CEO, he is also Chairman of the Board) will receive and consider reports on particularly significant changes that may present risk to the organization. Before starting cooperation with high risk Clients the consent of MLRO must be obtained to enter into a business relationship with such Clients or to continue business relationship with such Clients and the consent of MLRO must be approved by Director of Intstitution (CEO).

Head of Legal, Compliance and Risk Management is Board member who is responsible for AML CFT in the Institution and MLRO must be notified in writing the Financial Crime Investigation Service no later than 7 business days after their appointment or replacement.

The employees of the Institution (clients managers) is the first line of defence, are accountable for the AML/TF risks and risks related to financial crime.

The MLRO and employees from compliance team as the second line of defense, is responsible for the monitoring, assessment, guidance and reporting of money laundering, terrorist financing and financial sanctions risks.

Internal control officer (internal auditor) – as the third line of defence – is responsible for carrying out independent testing of the Institution's policies, procedures and controls.

Outsourcing to external suppliers (client identification, screening, information checking, other compliance/AML risk management services) may only be executed after close consultation with MLRO.

VI. Risk tolerance

The Institution does not tolerate any breach of the requirements set in this Policy that could damage the public trust and confidence in the company. Any material or systemic breaches must be reported to the MLRO. The Institution does not accept any business relationship with a designated person, group and entity subject to financial sanctions. In order to comply with financial sanctions regulations, the Institution verify the identity of its clients and beneficiary owners. Therefore the Institution requires a robust control environment with low error rates for due diligence after applying internal controls. Should a conflict arise between the requirements within this Policy and any other Policy/Procedure or legal requiremnt, MLRO shall be consulted. The Institution will take all relevant steps to reduce the provision of products and services to natural persons and/or legal entities where the Institution has a reason to suspect that the natural person and/or the legal entity is or will use the Instituition's products and/or services for ML/TF or financial crime.

VII. Client due diligence

The Institution's goal of developing its knowledge of its clients so as to improve the value of advice it can offer is closely related to the due diligence obligations of the Institution. In parallel to the verification of a client's identity, the Institution applies a risk based approach towards the collection, registration, and monitoring of information in relation to the nature and intent of the client relationship.

The Institution shall apply a risk based approach towards due diligence with reference to a client's geographic ties, chosen products and / or services, delivery channels and client specific factors. The Institution will decide upon appropriate client acceptance instructions in order to set clear guidance as to which natural persons and legal entities the Institution will see as the strategic client base with references to AML CTF and financial sanctions risk. The Institution requires a robust and effective IT solution to cater for an effective initial registration and ongoing monitoring of the client base. All clients - natural persons and legal entities - are registered on the Institution's IT (core) system. Having sufficient identification information, the Institution will - within the purpose of the requirements - aggregate all relevant products and services for each client. The Institution must identify and verify the identity of any natural persons who ultimately owns or controls the client.

Ongoing Due Diligence (ODD) means monitoring client relationships on a periodic basis, keeping a record of the measures taken to monitor the relationship and the information obtained, keeping a record

of the purpose and intended nature of the business relationship and reviewing and updating this information periodically.

Ongoing due diligence is an ongoing process where internal systems and controls are being used to monitor customers activity, which includes but not limited to:

(A) monitoring of transactions to identify activity that is inconsistent with employees' knowledge of the client and business relationship;
(B) screening of client, the representative person (manager), beneficial owner and associated party against sanctions and PEP lists on accurate and up to date information and record the finding results;
(C) reviewing client identification records and keeping information about the client up to date.

As part of ongoing due diligence, Institution will initiate client review if one the following, but not limited triggers occurs:

(A) client, representative person (manager) or beneficial owner or an associated party is newly identified as being a PEP;
(B) unusual activity notification or negative information about the client (beneficial owner) is received;
(C) when there is a request from a competent authority;
(D) based on a concern arising from the outcome of the investigation of a transaction monitoring alert or screening result;
(E) to fulfil these obligations, transactions that are out of profile will be identified through both real-time and retrospective monitoring.

Institution's responsible person for compliance and/or customer monitoring shall track the source of customer's funds, especially high value transaction and third party sourcing on the basis of special IT system alerts. Following steps are taken, when required, to ensure the source of funds and to check the compliance with the Law:

(A) transaction listing is sought from clients wherein high value transactions are detected. These include first time customers as well as regular clients;
(B) inward funds received in clients' accounts from any third party source is verified;
(C) all such transactions on source of funds are tracked by the Compliance team and necessary details like statements and details of third party are sought from the customer via customer services;

After verification, the Compliance team clears the transaction for processing.

Risk scoring of the customer determines how frequently Institution will monitor each business relationship and how frequently that business relationship information is to be kept up to date. All client relationships need ongoing due diligence but high-risk clients will be monitored more frequently.

VIII. Screening of politically exposed persons

In order to ensure that all natural persons defined as politically exposed persons (PEPs) are identified and registered in the Institution's IT (core) system as such, a PEP screening process is conducted when natural persons and/or legal entities are on-boarded. Furthermore, the client database is screened for PEPs on an ongoing basis.

IX. Customer risk scoring, on-going due diligence and enhanced due diligence

When identifying whether there is higher risk of money laundering and/or terrorist financing, the Institution assesses at least the following factors:

1) **client risk factors:**

a. the business relationship of the client is conducted in unusual circumstances without any apparent economic or visible lawful purpose;
b. the client is resident in a third country (not EEA);
c. legal persons or entities not having legal personality are personal asset-holding vehicles;
d. a company has nominee shareholders acting for another person, or shares in bearer form;
e. business is cash-intensive;
f. the ownership structure of the legal person appears unusual or excessively complex given the nature of the legal person's business;

2) **product, service, transaction or delivery channel risk factors:**

a. a product or transaction might favour anonymity;
b. business relationships or transactions are established or conducted without the physical presence;
c. payments are received from unknown or unassociated third parties;
d. products and business practices, including delivery mechanism, are new and new or developing technologies are used for both new and pre-existing products;

3) **geographical risk factors:**

a. countries identified, on the basis of data of reports or similar documents by the Financial Action Task Force on Money Laundering and Terrorist Financing or a similar regional organisation, as having significant non-conformities with international requirements in their anti-money laundering and/or combating the financing of terrorism systems;
- countries identified as high – risk third countries specified by the European Commission and the FATF organization (www.fatf-gafi.org/countries/#high-risk) (natural persons residing in these countries or legal entities established therein);

b. countries identified, on the basis of data by governmental and universally-recognised non-governmental organisations monitoring and assessing the level of corruption, as having significant levels of corruption or other criminal activity;
c. countries subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations;
d. countries provide funding or support for terrorist activities, or have designated terrorist organisations operating within their country.

Clients are classified with a risk tier: low, medium (standard), increased (high risk) and prohibited. When a clients are identified as increased (high-risk), they are subject to appropriate enhanced due diligence measures.

For new clients, Institution performs a risk scoring before entering into the business relationship with a client. Institution shall perform risk scoring for existing clients on an ongoing basis.

The Institution performs on-going due diligence and enhanced due diligence measures proportionate with the risk of the client. Increased (high risk) clients will therefore be subject to enhanced due diligence and annual on-going due diligence. On-going due diligence processes will be applied to all existing clients within a longer specific period that will determine by whether they are scored as medium (standard) or low risk category.

X. Data quality

The Institution IT (core) banking solution must be designed to ensure that internal controls of client due diligence are maintained. This requires strong data quality and, where possible, automatic on-going due diligence between public registries and the Institution's IT (core) system in relation to client data.

XI. Clients activities monitoring

The Institution applies a risk based approach to client's activities monitoring. Activities monitoring is conducted in order to evaluate whether the activities of the client (the use of the products and/or services and/or the general behaviour) is consistent with the obtained information on the purpose and intended nature of the business relationship. As part of its activities monitoring, the Institution further investigates clients' activities that are deemed to be unusual or suspicious with regard to the stated position of the client or there is negative or contradictory information about the client's activity, reputation, etc.
Investigating and reporting of the unusual/suspicious activity to the MLRO - is achieved through staff training and awareness measures.

The Institution have procedures for monitoring for suspicious activity and will clearly specify the parameters and thresholds that are in place to trigger an investigation. These procedures and monitoring scenarious shall be regularly reviewed and updated to account for changes and enhancements to the monitoring rules program.

Transactions monitoring are real time and retrospective.

The Institution is using a combination of system alerts- retrospective monitoring and blocks - real time monitoring to facilitate effective transaction monitoring.

The ongoing monitoring of the business relationship includes:

- transactional review;
- keeping up to date documents collected during KYC and enhanced due diligence (EDD) processes.

Monitoring will be undertaken by the Compliance team, which is in charge of reviewing transactions flagged as suspicious by automatic alerts and also additional all transaction review conducted using daily lists of processed transactions.

In the case of suspension of the operation the investigation should be initiated in order to detect if there are any suspicious signs.

Retrospective monitoring:

- retrospective monitoring should be performed manually.
- the records should be generated and saved within the terms set in procedures;
- MLRO should apply and approve trigger and filter the operations.

Triggers used to indicate transactions and customers - generate alerts, that need to be reviewed and checked by Compliance team:

- the size of particular transaction;
- volume and number of transactions;
- frequency of transactions in particular period;
- geographies of activity - transactions received/sent from high risk countries with no reasonable explanation;
- structuring of transactions to avoid dealing with identification requirements or regulatory record- keeping and reporting thresholds;
- high increase in activity;
- networking rules- many to one and one to many scenarios;
- transit accounts;
- lower/equal amounts (50-500 euro) sent to countries associated with higher terrorism risk;
- transactions in relation to NGO (non-governmental organizations, charity organizations), aid collection.
- potential consumer networks - many to one and one to many scenarios.

MLRO will regularly review the above parameters to ensure they remain relevant. This review shall be a part of the yearly risk assessment exercise.

XII. Sanctions

In order to comply with sanctions imposed by the UN, EU, US and Lithuania state authorities relevant control procedures must be in place. The market areas of Institution activities is Lithuania and EU Member States and, as such, are obligated to follow EU regulation and, therefore, comply with EU sanctions. US sanctions regulations have a major impact on the Institution as well.

The Institution shall not establish and maintain any business relationships with entities (natural and legal persons) and shall not fulfil any orders/transactions when entities are subject to the financial sanctions of the UN, EU, US OFAC (Office of foreign assets control) and on US Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) list or Lithuania and any performance of any transactions with these entities shall be prohibited (freezing of monetary funds or economic resources, prohibitions of financial transactions).

The Institution has a screening solution, which is integrated in the Institution's IT (core) system and uses „Dow Jones Riskcenter" data base to ensure that the Institution is compliant with AML, CTF and financial sanctions regulations.

XIII. Transaction and client screening

The Institution conducts transaction screening on all transactions in relation to relevant lists of designated persons, groups and entities subject to financial sanctions.

The client screening solution ensures that all client registered in the Institution's IT (core) system, including natural persons, legal entities and their representatives and beneficial owners, are constantly screened against the relevant sanctions lists of designated persons, groups and entities.

Persons, groups and entities designated by the UN, EU, US or Lithuania state authorities shall be highlighted and may be subject to asset freezing with subsequent reporting to appropriate authorities. The Institution also will terminate or limit the services offered to clients natural persons and legal entities designated by OFAC.

XIV. Management information system, reporting

The Institution's Board must determine key performance indicators and develop management information requirements and processes to gain insight into, and satisfaction with, the effectiveness of the AML, CTF and sanctions compliance framework.

At least once a year MLRO shall report to the Institution's Board on the activities of implementation of measures for AML CTF risk management (including, but not limited to information on and changes in the level of the money laundering and terrorist financing risk posed by Institution; effective measures for risk management (reduction), information on irregularities identified in the implementation of internal control measures and tools in the area of AMP CTF prevention, etc..; The Board also annually reviews the results of the AML CTF risk assesment in the Institution and decides on additional measures required for acquisition and / or allocation of additional resources to manage emerging risks.

XV. Retention and record keeping

For the purpose of preventing, detecting and investigating unusual and suspicious client activities, the Institution must keep electronic records of all transactions and due diligence measures carried out in accordance with this Policy.

Records must be kept in a manner making information and documents available to all employees having appropriate access to the client in question (within the Institution's existing IT solution). Documentation/record must be stored in a paper or in electronic form :

- data of the registration logs specified for a period of eight years as of the closing date of transactions or the end of business relationship with the client;
- copies of documents verifying the client's identity, identification data of the beneficial owner, live video transmission (live video broadcast) record (remote client identification process), other data received during identification of the client, documents related to accounts and/or agreements (original documents) for a period of eight years as of the closing date of transactions or the end of business relationship with the client;
- correspondence related to the business relationship with the client for a period of five years as of the closing date of transactions or the end of business relationship with the client;
- documents confirming the monetary operation or transaction and data or other instruments with legal effect, and data related to performance of the monetary operations or conclusion of the transactions for a period of eight years as of the date of performance of the monetary operation or conclusion of the transaction;
- letters by which findings of the investigation on operations that, by virtue of their nature, may be related to money laundering and terrorist financing, and complicated and unusually large transactions in particular, as well as any unusual transaction structure that does not have an evident economic or visible legal goal, and business relationship or monetary operations with clients from third countries that, pursuant to official information from inter-governmental organizations, do not enforce adequate money laundering and terrorist financing prevention measures or enforce measures that are not aligned with the international standards. The results of investigation of the grounds and purpose of such monetary operations shall be documented in writing and stored in paper or electronic form for a period of five years;
- all MLRO reports to the CEO and the Board will be kept indefinitely;
- the Institution maintains records of all AML training undertaken by empoloyees, the date it was provided and the results of any tests if applicable. These records will be kept for 10 (ten) years following the end of employment with the Institution;
- all SARs submitted including correspondence with the Financial Crime Investigation Service, the Bank of Lithuania (or any other government agency) will be kept for an unlimited period of time. Internal reports of suspicions will be kept for 10 (ten) years;
- the time limits for record keeping may be extended additionally for no longer than two years upon a reasoned instruction of a competent authority.

XVI. Training, awareness

The Institution has a training program for all employees to make sure that those who have contact with customers, who see client transaction activity client identification and record keeping requirements.

All new employees of the Institution are required to complete anti-money laundering and terrorist financing compliance training within their induction training period when they first join the Institution. All employees, acting as a first and second lines of defence, will also be enrolled and undertake the comprehensive and regular anti-money laundering and counter-terrorist financing training within their first 3 months of employment with the exception applicable to the employees who are directly involved in application of the AML CTF measures (such as the Compliance Manager) who must be introduced to the procedures of the Institution before they will start performing functions with relation to AML CTF.

Training is currently conducted through an internal customized course and the Institution also makes use of publicly available courses and material and purchased courses and materials particularly in certain specialist areas. The training program will be in writing but can be delivered electronically (via email and online forms) or by other means. The training program will be reviewed and updated by the MLRO to reflect requirements. Currently the compliance training includes a main training course with a test which everyone must complete.

To ensure employee training is kept up to date, all existing employees will receive follow up training on new and existing AML CTF and regulatory requirements on a regular basis (at least within one year of their last training). If the online training test results show that a staff member does not understand the training material, the Institution will ensure that the employee receives specialized one-on-one training to understand the AML CTF material.

An employee log of assigned and completed training materials shall be kept up to date by the MLRO and on file for five years (e.g. extract or download of training logs).

Relevant compliance training is for all employees. This includes those persons in sales and in senior management (Director, the Board members etc.) and others who have responsibilities under the compliance regime, such as information technology and other staff responsible for designing and implementing electronic or manual internal controls. The MLRO review functions and arrange to provide suitable and customized training.

The Institution training will include at a minimum:

- an understanding of the reporting, customer identification and record keeping requirements as well as penalties for not meeting those requirements;
- making all employees aware of the internal policies and procedures for deterring and detecting money laundering and terrorist financing that are associated with their jobs;
- delivering to employees a clear understanding of their responsibilities under these policies and procedures;
- all those who have contact with customers, who see customer transaction activity, who handle funds in any way or who are responsible for implementing or overseeing the compliance regime must understand the reporting, customer identification and record keeping requirements;
- making all employees aware of how the Institution is vulnerable to abuse by criminals laundering the proceeds of crime or by terrorists financing their activities;
- making all employees aware that they cannot disclose that they have made a suspicious transaction report, or disclose the contents of such a report, with the intent to prejudice a criminal investigation, whether it has started or not;

- that all employees understanding that no criminal or civil proceedings may be brought against them for making a report in good faith;
- background information on money laundering so everyone who needs to can understand what money laundering is, why criminals choose to launder money and how the process usually works;
- details of what terrorist financing is and how that process usually works;
- real-life money laundering schemes (preferably cases that have occurred at the Institution or at similar institutions), including how the pattern of activity was first detected, its impact on the institution, and its ultimate resolution.

MLRO is responsible for ensuring that everyone is periodically informed of changes in AML CTF legislation, policies and procedures, and current developments in money laundering or terrorist activity financing schemes particularly relevant to their jobs.

Certain employees, such as those in Compliance team, customer services and operations, require types of specialized additional training which will be provided either through external services or internally. The training program will be reviewed and updated to reflect requirements.

XVII. Review

This Policy must be reviewed by MLRO at least annually. Any changes to the Policy must be approved by the Board.

Binding document: „Client identification („Know Your Client“/KYC) procedure“ , „Procedure of implementation international sanctions“, „Procedure for assigning customers to risk categories and AML/CTF risk scoring”.