UAB “CORPORATE SERVICES”
ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING POLICY

Table of Contents

22
Corporate Services UAB Anti-Money Laundering and Counter-Terrorism Financing Policy approved by Management board on 9th of September 2020, decision No. 2.

I. INTRODUCTION

1. UAB "Corporate Services" (hereinafter the Company) is committed to conduct business operations in a transparent and open manner consistent with its regulatory obligations.

2. The Company is established as an electronic money institution which provides electronic money services.

II. SCOPE OF THIS POLICY

1. The aim of the Anti-Money Laundering and Counter-Terrorism Financing Policy (hereinafter the Policy) of the Company is to set out the following:

1.1. general principles, rules and responsibilities, and the main processes by which money laundering and terrorist financing (hereinafter ML/TF) risks are to be identified, managed and controlled in the Company;

1.2. rules and responsibilities, procedures used to determine the identity of the Company's customers when providing payment services in order to prevent ML/TF;

1.3. rules and responsibilities of the suspension of the transactions of the customers of the Company;

1.4. procedure, rules and responsibilities for provision of information about suspicious transactions to the Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania (hereinafter the FCIS);

1.5. training of employees of the Company;

1.6. reporting to the management of the Company about risk and accidents related to ML/TF.

2. All employees, including full-time, temporary or part-time employees, interns or contractors who have the access to information or tools, or are involved in the processes described in this Policy, are expected to be familiar with this Policy as it relates to their responsibilities, and act in accordance with its provisions.

3. This Policy is approved by the Board of the Company and must be reviewed at least annually or more frequently if an event requires a change to the Policy. Compliance Officer must conduct the annual review and update as appropriate to reflect changes in applicable AML/CTF laws and regulations or risk management practices.

III. GOVERNANCE, ROLES AND RESPONSIBILITIES

1. Effective AML/CTF risk management requires proper governance and the establishment of clearly defined roles and responsibilities across the Company.

2. The Company will ensure that responsibilities for AML/CTF and sanctions risk management are clearly defined and documented in role/job profiles and apportioned appropriately.

3. **Management Board**

3.1. The Management Board shall approve the Policy, as well as the results of the annual risk assessment.

3.2. The Management Board shall appoint the AML/CTF responsible Member of Board who is responsible for:

i organizing AML/CTF measures laid out in the applicable local and international legislation,
ii general oversight of the function,
iii understanding related operational risks,
iv helping to maintain its integrity and sufficiency,
v in accordance with prescribed terms of reference, participate in managing AML/CTF risk of the organization (eg. Committees, Board meetings)
vi receive regular risk updates from Company's AML/CTF responsible employee.

4. **The General Manager**

4.1. The General Manager of the Company is responsible for ensuring that the Company is fully equipped with the necessary resources to effectively manage and control its ML/TF risks at every organizational level and must communicate the importance of AML/CTF compliance to the organization.

4.2. The General Manager will determine and review the Company's AML/CTF risk assessment and financial crime risk appetite and will ensure resources are allocated to effectively manage and mitigate ML/TF risks across the Company in line with risk-based approach.

4.3. The General Manager will mandate the Compliance Officer to be accountable for the design and maintenance of effective AML/CTF and sanctions compliance system and control requirements, have adequate and competent resources as well as access to information to fulfil this function.

4.4. The Company shall have governing and decision-making committee to address AML/CTF risk management matters including prioritization of risk management activities, allocation of necessary resources, customer acceptance and customer termination where required.

5. **Compliance Officer**

5.1. The General Manager will mandate the Compliance officer to be accountable for the design and maintenance of effective AML/CTF and sanctions compliance system and control requirements, have adequate and competent resources as well as access to information to fulfil this function. The Compliance Officer is responsible for the listed below:

i. to receive disclosures from employees (hereinafter SARs);
ii. to decide if disclosures should be passed on to FCIS;
iii. to review all new laws and decide how they impact on the operational process of the Company;
iv. to prepare a written procedures manual and make it available to all staff and other stakeholders;
v. to make sure appropriate due diligence is carried out on customers and business partners;
vi. to keep and review records of all decisions relating to SARs appropriately;
vii. to ensure that staff receive appropriate training, when they join and that they receive regular refresher training on an annual basis or if necessary;
viii. to monitor business relationships and record reviews and decisions taken; ix. to make a decision on continuing or terminating business relationship with a particular customer.

6. Management information reporting

6.1. Senior management will be informed by periodical reports on compliance by the Compliance officer, which may include, but is not limited to:

i. practical situations of suspicious transactions, problematic customers, internal investigations and their outcomes;
ii. statistical information captured by the monitoring systems, numbers of suspended suspicious transactions, suspicious activity reports, numbers of transaction monitoring generated alerts;
iii. implementation of new regulatory requirements;
iv. recommendations to improve risk management, evaluation of effectiveness of monitoring;
v. other relevant information which would support decisions regarding resources and improvement of risk management controls.

6.2. When evaluating submitted reports, Senior management can make additional decisions on the reports provided and periodical evaluation of processes and controls of AML/CTF risk management.

IV. AML RISK ASSESSMENT AND RISK-BASED APPROACH

1. Key element of the risk-based approach is to identify and assess the risk of ML/TF posed by the customers to the Company.

2. The ML/TF risk assessment consists of the following steps:
2.1. to identify the ML/TF risks that are relevant to the business of the Company;
2.2. to carry out periodic risk assessments on various parts of our business, focusing on customer behaviour, delivery channels, patterns, irregularities;
2.3. to design and put in place effective controls to manage and reduce the impact of the risks;
2.4. to monitor the controls and improve efficiency;
2.5. to maintain records of processes/systems that were checked and why we checked them.

3. All customers should be reviewed in a ML/TF assessment process in respect of potential risks on money laundering and terrorist financing proceeds of crime and associated risks which have been set out.

For this purpose, Company implements a customer ML/TF risk assessment methodology which considers:

i. The geographical location where the customer operates (country, region, etc.),
ii. Certain products and services provided to the customer,
iii. Whether the customer is a politically exposed person[1] or not
iv. Business sector of the customer or the industry that the customer operates,
v. Type of transactions performed by the customer,

This methodology is revised by the Company when a new specific ML/TF risk related to a customer / certain transaction occurs.

4. ML/TF risk assessment is planned to be conducted annually or if there is a material change in the risk profile of the Company. The results of the annual ML/TF risk assessment should be presented and approved by the Management Board. The annual ML/TF risk assessment will be used to improve or optimize the existing processes and controls in the areas of the highest risk.

5. Implementing risk-based approach for the Company:
5.1. applies due diligence at the start of customer engagement by identifying and verifying the customer identity based on documents, data or information obtained from a reliable and independent source;
5.2. identifies where there is a beneficial owner who is not the customer, the beneficial owner and taking adequate measures, on a risk sensitive basis to verify his identity (including in the case of a legal person, trust or similar legal arrangement, measures to understand the ownership and control structure);
5.3. creates policies and procedures that relate to customer due diligence, ongoing Monitoring, internal reporting and record keeping;
5.4. if any suspicions are identified, then these should be raised to the Compliance officer for further investigation by completing the relevant internal SAR form.

V. KNOW YOUR CUSTOMER

1. Know Your Customer (hereinafter KYC) measures are applicable to all customer relationships and are proportionate to the risk they present.

[1] Under the Directive, including heads of states and governments, ministers, members of parliaments and of legislative bodies, members of governing bodies of political parties, members of supreme courts and high judiciary bodies, members of the diplomatic corps, individuals managing or supervising state-owned companies, members of international organizations and their family members.

2. KYC measures include:
2.1. Customer due diligence (hereinafter CDD);
2.2. Enhanced due diligence (hereinafter EDD);
2.3. Ongoing due diligence (hereinafter ODD), periodic reviews and monitoring;
2.4. Customer risk assessment.

3. KYC must not be seen as a process or a "checklist" exercise to simply collect customer information. In addition to customer information gathering, KYC enables each customer relationship to be fully assessed and the financial crime risk fully understood to determine if the risk presented is acceptable for the Company.

VI. KEY REQUIREMENTS AND PRINCIPLES FOR CUSTOMER IDENTIFICATION

1. When assessing the ML/TF risk the Employee aims to establish and assess the following circumstances:

1.1. **type of the customer**, i.e. whether a prospective customer has an ordinary business model such as e-commerce web sites who sell electronics, clothing, gifts, foods, accessory, furniture etc.; if not, the additional clarification and/or documentation must be requested from the customer seeking to establish if there is a high ML/TF risk; special attention to the following circumstances which may increase the ML/TF risk should be given:
i. if the customer is a Politically Exposed Person (hereinafter PEP);
ii. where the prospective customer is registered under the address which serves as a registration address for several companies;
iii. where the same person acts as a managing director or a Beneficial owner for several companies (save the large corporate groups);
iv. where the prospective customer is a non-profit institution ("NPI");
v. other circumstances indicated in these Procedures.

1.2. **commercial relationships**, i.e. assessing if the behavior of a prospective customer reveals that the aims and duration of the relationship expected by a prospective customer may considerably differ from what is inherent to an ordinary business model such as e-commerce web sites who sell electronics, clothing, gifts, foods, accessory, furniture etc.; if yes, the additional clarification and/or documentation must be requested from the customer seeking to establish if there is a high ML/TF risk; in addition it needs to be established, if the customer acts as a principal or is represented by the third person (agent) or otherwise applies on non-face-to-face basis which always increase the ML/TF risk of the customer.

1.3. **product**, i.e. assessing if the payment services in which a prospective customer is interested correspond to the nature of the business and the Transaction profile of such prospective customer; if not, the additional clarification and/or documentation must be requested from the customer seeking to establish if there is a high ML/TF risk; you should also draw your attention where the customer or the potential customer is to transact in new or developing technologies which may give rise to a threat of ML/TF or the use of Transactions that might favour anonymity;

1.4. **territory,** i.e. assessing where the main place of interests of a prospective customer is situated, e.g. where the customer is living/incorporated or where the place of the main business activity of the customer is situated or where the main part of the customers of the customer comes from; it is important to establish if such main place of interests of the customer is situated in the country other than FATF country (http://www.fatf-gafi.org/countries/#FATF) or in the Target territory; in such event the customer has to be considered as a high risk client.

2. Authorized employees must assess the above circumstances, indicated in above, and inform the Compliance officer and decide whether to **refuse accepting the Business relationship with such potential customer** or, if decided to further proceed with the due diligence procedure, **the enhanced due diligence must be applied**.

3. The Compliance must assess the above circumstances and decide whether to **refuse accepting the Business relationship with such a potential customer** or, if decided to further proceed with the due diligence procedure, **the enhanced due diligence must be applied**.

4. Only those customers for whom the legitimacy of the acquisition of assets and funds raises no doubt are acceptable to the Company. For this reason, it is important for the Company's employees to know the identity of the customer, which is why they must follow the principle of "Know your customer" in their activities.

5. In order to know its customer, the Company collects and analyses the following information about the customer:
5.1. where funds are transferred from to the customer's account and where the customer transfers funds to;
5.2. how often specific operations are carried out;
5.3. what currency each given operation is carried out in;
5.4. which operations the customer performs most frequently;
5.5. other similar information which helps to create a "portrait" of the customer – to know the customer. The customer "portrait" is created to identify the operations typical of the specific customer.

6. The Company is prohibited to conclude any agreements with the customers and has the right to refuse service and to unilaterally terminate its services, in cases when a natural or legal person or beneficiary if they:
6.1. did not provide, at the Company's request, all the information or documents required to identify the person or did not provide full requested information;
6.2. did not provide the Company with sufficient evidence or documents proving the origin of their assets, or if there is a reason to suspect that the person is engaged in money laundering or is using persons or companies whose shares are only quoted on stock exchanges, but which do not engage in any practical activities (business);
6.3. trying to hide the identity of the beneficiary or trying to avoid providing the information which is necessary to identify the beneficiary;
6.4. gave false information about themselves and/or their activities or intentionally concealed certain information or refused to submit it according to the Rules established by the Company and/or the legislative requirements of the Republic of Lithuania;
6.5. has or had connections/links with organized criminal organizations (according to reliable information collected by the Company from mass media or competent national authorities or provided by international organizations/institutions);
6.6. are associated or were associated in the past with traditional sources of revenue received from organized crime (e.g. smuggling of drugs or excise goods, illegal trade in arms or human organs; trade in prostitution services; the management of brothels; international money transfers without the appropriate permits (such as e-gold); underground banking (such as Hawala); lotteries, betting, or casino operation without permits from competent public authorities);
6.7. are included on the list of persons suspected of local or international terrorism or terrorist financing (e.g. cases when the United Nations General Assembly, the Organization for Security and Co-operation in Europe or other international organizations which the Republic of Lithuania is a member of or which the Republic of Lithuania participates in adopting appropriate decisions which recommend that international sanctions be imposed on certain subjects and the Republic of Lithuania implements them);
6.8. are persons subject to international financial sanctions (United States, United Nations and/or European Union, etc.);
6.9. caused, through unlawful actions, direct/indirect losses, or the real possibility of such losses to the Company

or harmed the reputation of the Company.

7. The Company has the right to refuse to provide services and/or to enter contracts with customers for the provision of services for other justified reasons, especially if the conclusion of certain contracts is impeded by legal reasons, such as limited or restricted capacity or the absence of representation rights.

VII. CUSTOMERS CATEGORIZATION AND STATUSES

1. Customers of the Company will be classified according to their risk level:
1.1. Low Risk;
1.2. Medium Risk;
1.3. High Risk.

2. The Company shall classify the customers into different levels according to the level of risk.
3. In determining a risk assessment for a customer, the presence of one factor that might indicate higher risk does not automatically establish that a customer is of higher risk. Equally, the presence of one lower-risk factor should not automatically lead to a determination that a customer is of lower risk.

4. The Company, when assessing whether there is a high ML/TF risk must evaluate at least these factors:

4.1. **Customer's attributes:**

i. the customer's business relations are carried out in unusual circumstances without an obvious economical or visual lawful purpose;
ii. the customer lives in a third country;
iii. legal persons or subjects that do not have a legal person's status carry out activities of a personal asset management company;
iv. the company has formal shareholders acting for another person or the company has got bearer form shares;
v. cash dominates the business;
vi. the legal person's ownership structure appears unusual or too complicated taking in context the activities of that legal person.

4.2. The features of a product, service, transaction, or service provider channel:

i. the product or transaction may create favorable conditions for anonymity; ii.
business relations or transactions are made or carried out without physical presence;
iii. payments are received from unknown or unrelated third parties;
iv. the product or business practice including service provision mechanism are new, also the use of new or developing technology while working with new or with old products.

4.3. Territorial characteristics:

i. based on financial action task force is to combat money laundering and terrorist financing or a similar nature regional organization's reports or data from similar documents significant inconsistencies between the system for combating money laundering and terrorist financing and international reequipments in a country are detected;
ii. based on governmental or universally recognized non-governmental organizations that monitor and evaluate the level of corruption data in the country there is an estimated high level of corruption or other criminal activity;
iii. the country is sanctioned, there is an embargo or similar measures declared by, for example, the European Union or the United Nations;
iv. the country finances or supports terrorist activities or in the territory of the state terrorist organizations act that are included into the list drawn up by international organizations.

VIII. CUSTOMER DUE DILIGENCE

1. Described due diligence measures must be performed at the start of each customer relationship with the Company.

2. Establishment of the identity of the customer and the beneficial owner is the process of the collection and verification of personal information about the customers and their representatives, where applicable.

3. The purpose of the Customer Due Diligence (CDD) process is to collect, process, verify and keep the information about the customers, due to minimize the possible and potential ML/TF risks.

4. For all customers CDD must be completed prior to entering the relationship and it is necessary to complete the steps as follows:
4.1. to perform identification and verification – identify and verify the identity of the perspective customer and related parties;
4.2. to screen all customers and related parties against the EU sanctions list and OFAC SDN list, UN list;
4.3. to screen all customers and related parties to determine if there are any PEPs associated with the customer and related party (beneficiary) and if they are PEP's themselves, by using public, trustworthy, and open information source;
4.4. to determine customer risk rating;
4.5. to complete Enhanced Due diligence (EDD) as required by the risk rating.

IX. MINIMUM INFORMATION TO CREATE CUSTOMER'S FILE

1. When conducting CDD, a minimum of personal information about the customers and their representatives must be collected, i.e.:

1.1. In case of natural persons, an identity document of the Republic of Lithuania or a foreign state or a residence permit in the Republic of Lithuania which contains the following data confirming person`s identity: i. name/names;
ii. surname/surnames;
iii. personal number (in the case of an alien – date of birth (where available – personal number or any other unique sequence of symbols granted to that person, intended for personal identification), the number and period of validity of the residence permit in the Republic of Lithuania and the place and date of its issuance (applicable to aliens);
iv. photograph;
v. signature (except for the cases where it is optional in the identity document);
vi. citizenship (in the case of a stateless person – the state which issued the identity document).

1.2. In case of legal entities, the identity documents, or copies thereof with a notarial certificate, confirming the authenticity of the copy of the document, which contain the following data:
i. name;
ii. Legal form, registered office/address, address of actual operation; iii. registration number (if such number has been issued);
iv. an extract of registration and its date of issuance;
v. beneficial owner`s name and identification details;
vi. ownership memorandum, article of association etc.;

vii. other relevant documentation such as company's activity details, expected turnover; viii. expected type and volume of transactions;
ix. main counterparties and countries;

2. Where the customer is a legal person represented by a natural person, the identity of the representative shall be established in the same manner as the identity of a natural person. The customer must also provide information about the director of the legal person: his name, surname, personal number (in the case of an alien – date of birth (where available – personal number or any other unique sequence of symbols granted to that person, intended for personal identification), his citizenship (in the case of a stateless person – the state which issued the identity document).

3. Where a customer is a legal person represented by a natural person, the Company requests from him a power of attorney (hereinafter POA) and verifies its validation (i.e., the issuing person's right to issue such POA), expiration date of such POA, what kind of actions are specified to be made in the POA (POA must meet the requirements set. POA issued abroad must be legalized or approved by a document confirmation certificate – apostille).

4. The Company will require a government issued ID with prospective customer photo to verify his/her identity.

5. The Company will require officially certified copies of provided documents.

6. Before and during the on-boarding of the customer responsible employees will:
6.1. assess if customer or representative presents valid identification documents;
6.2. assess if the photograph presented in the document is of that particular customer;
6.3. find out if a customer as a private or legal person will use the services directly or will represent the interest of another person;
6.4. make sure that necessary POA to act on behalf of customer is provided;
6.5. check if there are any circumstances to apply EDD.

7. For verification purposes the Company will use reliable and independent sources (national company registers or KYC related WEB products)
8. Every customer shall be verified if he/she is not included in Consolidated Persons list, its groups, company's list to which US, UN and EU sanctions are applicable , as well if the client does not have an interface with countries subject to EU sanctions, as well as countries classified as high risk or noncooperating according to the FATF.

X. BENEFICIAL OWNERSHIP

1. When establishing the customer's identity in all cases it is mandatory to identify the beneficiary(s). The identification of the beneficiary in all cases means the identification of a natural person or a group of natural persons.

2. Beneficial owners are considered the individuals who own, either directly or indirectly, a shareholding of at least 25% plus one share or has an ownership interest of more than 25% in the customer. There may be situations where it is impossible to identify who ultimately owns or carries out control over a legal entity. After using all possible means of identification, beneficial owner should be considered the individual who holds the position of senior manager in the legal entity.

3. Where the identity of the customer is established without the physical presence of the customer, the customer that is a natural person or a representative of the customer that is a legal person must submit the data on the beneficial owner:

3.1. First name;
3.2. Last name;
3.3. Personal identification code when available (in other cases date of birth);
3.4. Citizenship (if a person does not have a nationality – country that issued the person identifying document).

4. The data submitted by the customer shall be validated using electronic identification means issued in the European Union which operate under the electronic identification schemes with the assurance levels high or substantial, or with a qualified electronic signature supported by a qualified certificate for electronic signature which conforms to the requirements of the European Parliament's and of the Council's regulation (EU) No. 910/2014 of July 23rd, 2017 (hereinafter the Regulation), or using electronic means allowing direct video streaming.

5. The Company collects and when requested by the FCIS provides this information about the beneficiary:

5.1. beneficiary's identity data;
5.2. proof of information's provided by the customer checks in reliable and independent sources;
5.3. data about the customers (legal person's) management structure.

6. The Company checks the customer's provided data and information about the beneficiary, based on the documents, data, or information that it received from a reliable and independent source. The Company`s actions include a request to the customer to indicate public sources in which the information about the beneficiary may be verified.

XI. NON FACE-TO-FACE CUSTOMERS

1. All customer relationships identified by using non-face-to-face identification method. This also applies to those cases where the customer, either natural or legal person, is represented by another person.

2. The Company will ensure compliance with the rules for the customer's and beneficial owner's identity establishment without their physical presence by implementing the following measures:

2.1. by using third party information about the customer or the beneficiary in accordance with the article 13 of the Law of the Republic of Lithuania on the Prevention of Money Laundering and Terrorist Financing (hereinafter the Law);
2.2. by using electronic identification means issued in the European Union which operate under the electronic identification schemes with the assurance levels high or substantial, as specified by Regulation;
2.3. when information about a person's identity is confirmed with a qualified electronic signature supported by a qualified certificate for electronic signature which conforms to the requirements of Regulation. Third country's qualified electronic signatures supported by a qualified certificate for electronic signature are recognized according to article 14 of the Regulation;
2.4. by using electronic means which permit live video transmission in one of the following manners:

i. during the live transmission, a document proving the identity or a corresponding permits to residence in Lithuania original is captured and the identity is confirmed by using at least an advanced electronic signature that meets the requirements set in article 26 of the Regulation;
ii. during the live transmission, the customers facial image and document proving the identity or a corresponding permit to residence in Lithuania original are recorded.

3. When establishing the identity of the customer and beneficiary without the customer's physical presence the Company must verify the customer's and beneficiary's identity, receive data specified in this Policy which is used

to establish the customer's and beneficiary's identity data, documents or additional information that would allow to be sure of the customer's identity authenticity, to check whether there are circumstances to apply the enhanced identification of the customer's identity.

4. The Company is held responsible for following the rules of customer's and beneficiary's identity establishment without their physical presence.

XII. ENHANCED DUE DILIGENCE

1. Enhance due diligence (EDD) refers to situations where a customer presents a higher risk of financial crime and standard evidence of identity may be insufficient. Additional information needs to be obtained to assist with the customer approval and monitoring processes. EDD measures must be applied in addition to the regular CDD, which include, but are not limited to:

1.1. Verification of customers, its beneficial owners and associated parties using reliable and independent sources;
1.2. Verifying source of funds and source of wealth of the customer;
1.3. Screening all high-risk customers and their associated parties for adverse media;
1.4. Obtaining and assessing information on the purpose and intended nature of the relationship to understand why the customer is establishing a relationship with the Company;
1.5. Obtaining and assessing information for unusually high/frequent transactions;
1.6. Reviewing funding sources used for conducting transactions.

2. Enhanced customer identification is done by using additional means for establishing the customer's and beneficiary's identities:

2.1. when transactions or business relations are made with PEPs;
2.2. when transactions or business relations are made with natural persons that live or legal persons that are established in high risk third countries that are in the European Commission's and Financial action task forces to combat money laundering and terrorist financing published list of states that have serious flaws in preventing money laundering and (or) terrorist financing. After assessing the risk, the enhanced customer identification does not need to be applied for financial institutions or other affiliated entities or subsidiary companies that are established in the European Union in which they have a majority of shares and they are in a third country that the European Commission named as a high risk, if these branches and subsidiary companies follow the whole group's set requirements equal to requirements set by the Law;
2.3. if according to the Company's risk evaluation and management procedures a high risk of money laundering and (or) terrorist financing is determined. When evaluating the risks of money laundering and (or) terrorist financing it is necessary to evaluate the factors of possible high risks of money laundering and (or) terrorist financing.
2.4. in the cases set by the European supervisory authorities and the European Commission.

3. When performing an enhanced customer identification where transactions or business relations are carried out with politically exposed persons, the Company must:

3.1. establish and implement internal procedures according to whom it is determined whether the customer and beneficiary are PEPs;
3.2. receive approval from the senior manager to establish or continue business relationships with costumers when they become PEPs;
3.3. take appropriate measures to determine the source of assets and funds related to the business relations and transaction;
3.4. constantly perform an enhanced monitoring of business relations with PEPs.

4. When a PEP stops serving in an important public position, the Company for at least 12 months must consider the risk that that person still poses and to imply adequate measures to the risk level until it is determined that that person does not pose a risk inherent to PEPs.

5. When applying enhanced customer identification for natural persons living and established legal persons in countries that the European Commission and Financial action task forces to combat money laundering and terrorist financing has named as a high risk third countries also in those cases when the Company's risk evaluation and management procedures state a high risk of ML/TF the Company at its own discretion applies one or several additional measures to establish the customers and beneficiaries identity to lower the arising risk and must:

5.1. receive approval from the senior manager to establish or continue business relationships with these costumers;

5.2. respond appropriately to determine the source of the assets and funds related to business relations or transaction;

5.3. carry out a constant enhanced monitoring of the business relationship with these customers.

6. When applying enhanced customer identification, the Company in the cases set by the European supervisory authorities and European Commission chooses measures to undertake that are listed in the European supervisory authorities' and European Commission's documents in which these cases are listed.

7. The Company is forbidden to begin or continue correspondent banking or other relationships with a fictitious bank or a bank when it is known that that bank allows fictitious banks to use its accounts. The Company must apply measures that would allow to be certain that financial institutions that receive funds do not allow fictitious banks to use their accounts.

8. The Company must pay special attention to any risk of money laundering and (or) terrorist financing that may arise due to any type of product or other man made work result, use of provided services or ongoing transactions when there is an intention to conceal (leaning to anonymity) the identity of the customer or beneficiary, also regarding business relations or transactions with a customer whose identity was not established with his physical presence and, if necessary to immediately take measures to prevent the use of assets for ML/TF.

XIII. POLITICALLY EXPOSED PERSONS

1. A Politically Exposed Person ("PEP") is defined as an individual who is or has been entrusted with prominent public functions domestically or in foreign countries or by international organizations and/or their family members or persons to be known as their close associates of such persons. Such individuals who have, or have had, a high political profile, or hold or have held, public office, can present a higher ML/TF risk, as their position may increase their vulnerability to corruption, therefore such customers are always treated as a high risk.
2. The **PEPs** include, but are not limited to:

2.1. Head of the State, Head of the Government, Minister, Vice Minister or Deputy Minister, Secretary of the State, Chancellor of the Government, Parliament, or ministry;

2.2. Member of Parliament; Member of the Supreme Court, Constitutional Court, or any other highest judicial authority whose decisions are not subject to appeal;

2.3. Municipality mayor, director of a municipality's administration;

2.4. Member of the Management body of Lithuanian Chamber of Auditors or the Board of Central Bank;

2.5. Ambassador, charge d'affaires ad interim or high-ranking military officer;

2.6. Member of a management or supervisory body of a limited liability company, whose >50% shares or voting rights are owned by the state;

2.7. Member of a management or supervisory body of a limited liability company, whose >50% shares or voting rights are owned by the municipality;

2.8. Head of an international intergovernmental organization, his/her deputy, member of the management or supervisory body;
2.9. Leader of a political party, his deputy, member of the management body.
2.10. Immediate family members are spouse/partner, parents, brothers, sisters, children and children's spouses/partners.
2.11. Close associates are considered business partners or associates, especially those that share (beneficial) ownership of legal entities with the PEP, or who are otherwise connected (e.g., through joint membership of a company board).

3. The Company will assess the risks associated with PEP relationships before the beginning of the customer relationship and on ongoing basis by determining whether customer, beneficial owner or any associated party (family member or close associate) is a PEP.

4. In situations where PEP is identified, at least following minimum EDD measures must be applied:
4.1. Establishing understanding of wealth and verifying source of funds that are involved in customer relationship;
4.2. Conducting enhanced ongoing monitoring of customer relationship.

5. For the acceptance of PEPs, senior management approval hierarchy is organized in order to ensure that all new and existing PEP relationships are approved or re-approved based on the outcome of the EDD review. The decision and rationale for approval must be properly documented for each PEP.

6. Once an individual has been classified as a PEP, the status as a PEP must continue for a minimum period of 12 months after leaving the position meaning the same enhanced measures are applied for that timeframe. Senior management must in all cases approve declassification of a PEP where a new or existing customer is identified as a former PEP (when status was held more than 12 months ago).

XIV. ONGOING DUE DILIGENCE

1. Ongoing due diligence ("ODD") is an ongoing process where internal systems and controls are being used to monitor customers activity, which includes but not limited to:
1.1. monitoring of transactions to identify activity that is inconsistent with our knowledge of the customer and business relationship;
1.2. screening of customer, beneficial owner and associated party against sanctions and PEP lists on accurate and up to date information;
1.3. reviewing customer identification records and keeping information about the customer up to date.

2. As part of ongoing due diligence, the Company will initiate customer review if one of the following, but not limited triggers occurs:
2.1. customer or an associated party is newly identified as being a PEP;
2.2. unusual activity notification about the customer is received;
2.3. when there is a request from a competent authority;
2.4. based on a concern arising from the outcome of the investigation of a transaction monitoring alert or screening result.
2.5. to fulfil these obligations, transactions that are out of profile will be identified through both real-time and retrospective monitoring.

3. The company's person responsible for Compliance shall track the source of customer's funds, especially high value transaction and third-party sourcing based on system alerts. The following steps are taken, when required, to ensure the source of funds and to check compliance with the Law:

3.1. transaction listing is sought from customers wherein high value transactions are detected. These include first time customers as well as regular customers;
3.2. inward funds received in customers' accounts from any third-party source is verified;
3.3. 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;
3.4. only bank statement showing names of the account holder, bank code and listing of minimum two weeks is accepted for verification;
3.5. until the bank statement is received, customer transaction processing is put on hold by Compliance.

4. After verification, the Compliance Team clears the transaction for processing, otherwise the money is refunded.

XV. PERIODIC REVIEWS

1. Company updates data, documents and information about customers and beneficiaries on a regular basis to ensure that transactions comply with the Company's available information about the customer and to ensure that transaction comply with business risk and sources of funds.

2. Company shall update data about the client:

2.1. High Risk: reviewed every 12 months and EDD would be performed on a regular basis (Note. Review for all financial institutions for which a license is required (PSP, Crypto exchange, etc.), should be done every 6 month);
2.2. Medium Risk: reviewed every 24 months.
2.3. Low Risk: reviewed every 36 months.

3. The company must carry out permanent enhanced PEP monitoring.

4. If there is a change in data, documents or information about customers or beneficiaries, Company requires that the customer provide this information without delay.

5. In updating the above data, customers and beneficiaries must provide said data in the procedure established by Company and by the Law.

6. In all cases Company shall ask the customer to fill the questionnaire to prevent ML/TF in which following information shall be included:
6.1. Legal entities who directly control 25% or more customer's shares, voting rights, capital or equivalent (for legal persons);
6.2. Beneficial owner information – date of birth, address, name and surname, information regarding connections with PEPs (for natural persons);
6.3. Ownership structure, registration address, phone number, e-mail address, client's representative personal identification document and information about the person, main business partners list, main activity, financial indicators, turnover, services list company are planning to use (for legal persons);
6.4. Personal identification document, the purpose of the relationship, the nature of the relationship, the information about the person's activity and intense, information about connections with politically exposed persons (for natural persons).

XVI. INVESTIGATION AND REPORTING

1. All alerts generated by transaction monitoring system must be reviewed and investigated, and if required, escalated appropriately to the senior level employees. Responsible unit employees are responsible for obtaining

additional KYC information to review and investigate the alert thoroughly and determining whether the alert requires further escalation to senior level employees or to the Compliance Officer.
2. At the time of unusual or suspicious activity identification, responsible unit employees will contact the customer to request documentary evidence such as bank statement or legal documents or other documents to justify and evidence the reason behind identified unusual or suspicious transaction. When the responsible employees are not certain or sure, or if there is not enough justifying evidence about the authenticity and legitimacy of the transaction – the customer and unusual transactions must be escalated to senior level employees for further investigation or possible escalation to Compliance Officer for SAR reporting. All escalations rationale and background with related information must be documented and recorded on customer's record. It must be ensured that the KYC information held on the customer is updated and assessed to reflect relevant information obtained during the review and investigation.
3. Policy gives only general directions on investigation and reporting. For more detailed information see AML Procedure and TM Procedure.

XVII. SUSPICIOUS ACTIVITY

1. If applying all AML due diligence measures employee establishes that transaction being performed by the customer may be associated with ML/TF, the employee must immediately suspend the transaction except for cases when it is objectively impossible due to the character of transaction, their performance method, or other circumstances and escalate the customer or transaction to the Compliance officer with full details.

2. The Compliance officer must report to FCIS about suspicious or unusual ransaction or operation not later than within 3 business hours of the suspension of transaction or operation, irrespective of the amount of the operation or transaction.

1. FCIS may request to provide all necessary information which is needed to carry out the verification of the suspicious transaction. In such cases the requested information must be provided within 1 (one) business day after receipt of the respective request of the FCIS. FCIS must be urgently notified (no suspension is needed) if there is confirmed information that the customer intends or will attempt to perform a suspicious transaction.

2. FCIS may request to suspend the suspicious or unusual transaction performed by a customer. Responsible employees must, from the time specified therein or from the moment of emergence of specific circumstances, suspend the transactions for up to 10 (ten) working days.

3. Upon receipt of a written report from the FCIS that the suspension of a operation or transaction may interfere with the investigation of ML/TF and other criminal acts related ML/TF, the Company, after the receipt of a written notice or the moment specified therein, will not stop the suspicious transactions or transactions of the customers and the suspended transactions or transactions will be renewed immediately.

4. All internal enquiries made in relation to the report must be documented or recorded electronically. The Compliance officer should then scrutinize the escalated transactions, and if it proves positively suspicious – submit SAR to FCIS.

5. It is a criminal offence for anyone, following a disclosure to a nominated officer or to the appropriate institution, to do or say anything that might either "tip off" another person that a disclosure has been made or prejudice an investigation. When customer account is the subject of a SAR, there must be taken careful steps while communicating with customer and additional advice should be taken from the Compliance officer in order not to accidentally disclose investigative actions to the customer.
6. The Company must appoint senior executives who organize the implementation of measures for the prevention of ML/TF established by the Law and cooperate with the FCIS. The Company must also appoint a member of the board to organize the implementation of measures for the prevention of ML/TF as provided for in

the Law and senior staff members who cooperate with the FCIS. The appointment of such employees and members of the management board must be notified in writing to FCIS no later than 7 working days after their appointment or change.

XVIII. AUDIT, TESTING AND ASSURANCE

1. The Company will cooperate with an external audit company to perform an annual audit to test compliance with the Policy and related procedures. The audit will be performed annually, with necessary policy adjustments to follow in a timely manner. An official audit report will be produced and provided to the senior management including all findings and remediation actions by the 4th quarter of each year. In addition, the Compliance officer may on an *ad-hoc basis* and depending on the highest risk areas of the AML framework perform monitoring and testing of:

1.1. quality and effectiveness of internal AML controls and processes;

1.2. compliance with applicable AML/CTF laws and regulations, this Policy and accompanying procedures.

XIX. STAFF TRAINING

1. All staff, whether on a full-time, part-time or contract basis, are made aware of this Policy, manual and the obligations arising from them for both themselves and The Company provides training on anti-money laundering.

2. These training comprises two key elements:

2.1. Induction Training – the Compliance officer is responsible for identifying relevant new staff that are required to undertake induction training within 45 days after employment. The training is provided by the Compliance Officer, or the Compliance Officer will engage external AML Advisors and is face to face training. The content of the training includes awareness training, covering ML/TF. Understanding of the subject matter is assessed throughout the training through case studies. Until a new staff member has been signed off as competent no direct customer contact is allowed.

2.2. Refresher Training – all relevant staff must undertake face to face refresher training on an annual basis. The training is provided by the Compliance Officer, or the Compliance Officer will engage external AML Advisors and assessment of staff understanding is carried out throughout the training.

3. The Company will obtain acknowledgement from staff that they have received the necessary training by requesting staff to sign their attendance at training sessions. Overall monitoring of attendance is recorded manually and stored on the AML file. Certificate will be provided to each participant on successful completion.

XX. RECORD KEEPING

1. The Company must keep the following records:

1.1. **Customer Identification Records**:

i. All records of steps taken to obtain identification records, as well as copies of evidence of the identity of the customer as the case may be;

ii. All risk assessment records as well as the customer risk profile;

iii. A standard application form must be completed for every new customer as well as for the existing customer where the identification of the customer is needed under these Procedures; the filled application form must be signed off by all the clients and prospective clients;

iv. All records related to the ongoing monitoring of the clients.

1.2. **Money Laundering and/or Terrorist Financing Prevention Registers**

1.2.1. A Register of Suspicious Transactions;
1.2.1. A Register of the customers with Whom Transactions or the Business Relationship Have Been Terminated under the Circumstances referred to in Article 18 of the Law or under other circumstances related to infringements of the procedure of ML/TF prevention.
1.2.3. An Internal investigation register.

1.3. **Other Records**:

1.3.1.Evidence of the training programs on ML/TF prevention whether in-house or external;
1.3.2.. Evidence of the proper acknowledgment of the employees with these procedures and their amendments as may be needed from time to time.

2. Requirements for the administration of the register

2.1. The registers shall be managed and kept in an electronical manner.

2.2. The administrator of the Company's Registers and the person in charge of the provision of information to the FCIS shall be the Company's Compliance officer. The Company' Compliance officer shall be responsible for implementing and organizing ML/TF prevention measures provided for in the Law and for liaising with the FCIS.

2.3. Any other employees of the Company may use, change, or do any other action related to the Registers only upon prior written permission of the Company's Compliance officer and only provided that it is necessary for the urgent performance of the Company's activities, for the purposes of ML/TF prevention, and implementation of other requirements provided for in legal acts.

2.4. If the Company's General Manager authorizes and/or appoints other persons to be responsible for implementing and organizing ML/TF prevention measures provided for in the Law and for liaising with the FCIS, the Company's General Manager shall undertake to notify the FCIS to that effect separately.
2.5. The access to the Registers is granted to the Company's General manager, Compliance officer, or the person authorized by the latter. The possibility of destroying, changing, or using the data of the Registers must be restricted by a password known to the Company's Compliance officer or another authorized person. If the passwords for logging in to the Registers become known to any third parties, the Company's Compliance officer shall immediately take all measures to deny access to the Registers with the use of those passwords and, if the passwords become known, they must be replaced with new ones.
2.6. The Company's Compliance officer shall ensure that the data of the Registers are protected against unlawful destruction, change, or use.

2.7. Having established that transaction may be suspicious or unusual, having noticed indications of money laundering and/or terrorist financing, the employees of the Company must report such findings to the Company's Compliance officer, who shall register information about the client and transaction performed by him in the respective Register referred to in this Procedure, double-check the transaction and related information, and, where required, shall transfer the information to the FCIS in accordance with the mutually agreed procedures and form.

3. Completion of the register

3.1. The following data shall be entered in the General Money Laundering and/or Terrorist Financing Prevention Register:

i. Data proving the identity of the client and his representative (if the transaction is being concluded through a representative) (for a natural person – name and surname, date of birth, personal identification number, or another unique sequence of symbols assigned to that person intended for the identification of the person; for a legal person – name, legal form, registered office address, and code if such a code is assigned);
ii. Data on the transaction – the date of the performance of the transaction, the description of the property in respect of which the transaction is being concluded (money, real estate, etc.), and its value (the amount of money, currency in which the transaction is being performed, market value of the property, etc.);
iii. Data on the person who is the beneficiary of the funds (for a natural person – name and surname, date of birth, personal identification number, or another unique sequence of symbols assigned to that person intended for the identification of the person; for a legal person – name, legal form, registered office address, and code if such a code is assigned).

3.2. In the Register of Suspicious Transactions, in addition it shall be indicated which criterion approved by the FCIS, according to which it is identified that the transaction of the customer is considered as suspicious, is met by the operation or transaction.

3.3. In the Register of the customers with Whom Transactions or the Business Relationship Have Been Terminated under the Circumstances referred to in Article 18 of the Law or under Other Circumstances Related to Infringements of the Procedure of Money Laundering and/or Terrorist Financing Prevention, in addition the reasons for which the transactions or the business relationship has been terminated under the circumstances referred to in Article 18 of the Law or under other circumstances related to infringements of the procedure of money laundering and/or terrorist financing prevention shall be indicated.

3.4. Data shall be entered into the Registers in chronological order, on the basis of the documents confirming the transaction or other documents having legal force, which are related to the performance of transactions, immediately but not later than within 3 working days from the performance of the transaction.

4. Periods of and measures for the storage of information

4.1. The data of the Registers shall be stored for at least 8 (eight) years from the day of termination of transactions or other business relationship with the customer.

4.2. Documents confirming transaction or other documents having legal force related to the performance of the transactions shall be stored for 8 (eight) years from the day of the performance of the transaction.

4.3. Copies of the documents proving the client's identity, invoices and/or contractual documentation (original documents) shall be stored for 8 (eight) years from the day of termination of the transactions or business relationship with the client.

4.4. Written or electronic correspondence relating to the business relationship with the client shall be stored for 5 (five) years from the day of the termination of the transactions or business relationship with the client.

4.5. Results of investigations of complex or unusually large transactions and unusual transaction structures are stored for 5 (five) years in paper format or on an electronic medium.

4.6. The storage period may be extended additionally upon a reasoned instruction of a competent institution, nevertheless the extension cannot last longer than 2 (two) years.

4.7. The Company's Compliance officer must provide the stored documents to the FCIS or other institutions in case the latter request such documents in accordance with the procedure established by legal acts.