ANTI-MONEY LAUNDERING (AML)
AND
COUNTER TERRORIST FINANCING (CFT)
COMPLIANCE POLICY

HEDPAY UAB

VERSION 1.0

Document History

Version	Approval Date	Author	Change Status	Approved by
1.0	2020- 10 -10		First issue	CEO

1. GENERAL PROVISIONS

1. Hedpay UAB (hereinafter – the Company) is a virtual currency exchange company, acting according to the laws of the Republic of Lithuania. The Company is committed to conduct business operations in a transparent and open manner consistent with its regulatory obligations.

2. This policy implements the Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania, dated 19 June 1997 No VIII-275 No XIII-2584 (hereinafter – the Law).

3. The Company by implementing measures to prevent money laundering and / or terrorist financing is guided by the following main documents issued by the Director of the Financial Crime Investigation Service:

   - Technical Requirements for the Customer Identification Process for Remote Identification Authentication via Electronic Devices for Direct Video Transmission approved by the Director of the Financial Crime Investigation Service under the Ministry of Internal Affairs of the Republic of Lithuania on November 30th 2016 by Resolution No. V-314 “For the Technical Requirements for the Customer Identification Process for Remote Identification Authentication via Electronic Devices for Direct Video Transmission” (hereinafter – Technical Requirements).

   - Resolution No. V-240 of December 5th of 2014 of the Director of Financial Crime Investigation Service under the Ministry of Internal Affairs of the Republic of Lithuania "On the Approval of the List of Criteria for Money Laundering and Suspicious or Unusual Monetary Operations or Transactions Identification".

   - Resolution No. V- of 5 January 10th of 2020 of the Director of Financial Crime Investigation Service under the Ministry of Internal Affairs of the Republic of Lithuania “On the Approval of Guidelines for the Depositary virtual currency wallet operators and virtual currency exchange operators to prevent money laundering and/ or terrorist financing.”

   - Resolution No. V-273 of October 20th of 2016 of the Director of Financial Crime Investigation Service under the Ministry of Internal Affairs of the Republic of Lithuania “On the Approval of Guidelines for the Supervision of Financial Crimes for the Implementation of International Financial Sanctions in the Field of Regulations of the Ministry of Internal Affairs of the Republic of Lithuania.”

4. The supervisory authorities have the right to initiate inspections of implementation of the money laundering and/or terrorist financing prevention measures set out in the Law at their own initiative on the basis of the supervisory authorities' inspection plan (supervision plan).
5. The supervisory authorities may also initiate inspections relating to possible breaches of the Law upon receiving a report or any other data in which the circumstances of the possible breaches of the Law are recorded.
6. The following shall be considered as a serious breach of the Law:
    - failure to comply with the customer due diligence requirements;
    - failure to comply with the requirements for reporting of suspicious monetary, virtual currency exchange operations or transactions in virtual currency;
    - failure to comply with the requirements for the storage of information;
    - where an obliged entity have not put in place the internal control procedures.
7. The definitions used in this Policy are those defined in the Law.

2. ROLES AND RESPONSIBILITIES

The Board has a critical oversight role - as the senior-most management of the company, they should approve and oversee policies for risk, risk management and compliance. The Board also should have a clear understanding of the ML risks, including timely, complete, and accurate information related to the risk assessment to make informed decisions. Along with the General manager, the Board should appoint a qualified AML Officer with overall responsibility for the AML function and provide this senior-level officer with sufficient authority that when issues are raised they get the appropriate attention from the Board, the General manager and the business lines. The Board is responsible for the overall AML/CTF compliance policy of the Company and ensuring adequate resources are provided for the proper training of staff and the implementing of risk systems. The Board will receive and consider quarterly compliance reports presented by the AML Officer.

The General Manager will receive and consider the monthly compliance reports sent by the AML Officer and authorize changes based on the recommendations if required. General Manager will also receive reports on particularly significant changes that may present risk to the organization. Assistance may be given to the AML Officer in the preparation of the AML program.

The Compliance Officer is responsible for receiving internal disclosures and making reports to the Financial Crime Investigation Service (FCIS). First point of contact for all compliance issues from staff. Prepares monthly and quarterly reports for consideration to the General manager and the Board and conducts risk assessments of compliance systems. Undertakes regular random analysis of transactions including assessment of documentary evidence provided by Customers. Prepares any necessary amendments to AML/CTF Procedures Manual in line with risk assessment. Ensures everyone is periodically informed of any changes in anti- money laundering or anti-terrorist financing legislation, policies and procedures, as well as current developments and changes in money laundering or terrorist activity financing schemes particular to their jobs, constructing AML/CFT-related content for staff training programs. Reviews Customer identification information to ensure that all the necessary information has been obtained. First line of high-risk customers' approval. Establishes and implements the risk scoring matrix following regulatory guidance and for review and approval by the General manager.

Other staff members are responsible familiarize with this Policy, other internal procedures related to their job role and understanding responsibilities. Ensure AML/CTF procedures are adhered to. Ensure that all suspicious activity is reported to the AML Officer.

3. MEASURES TO PREVENT MONEY LAUNDERING AND/OR TERRORIST FINANCING

The Company implements these measures to prevent money laundering and / or terrorist financing:

1. Identification of the customer and beneficial owner:
    - determines whether the customer is acting on his own name or under control;
    - if the customer is acting through a representative, identifies customer's representative;
    - identifies customer (natural person);
    - identifies customer (legal entity);
    - identifies customer's (legal entity) beneficial owner;
    - collects information about customer's (legal entity) director;
    - collects information on the ownership and management structure of customer legal entity, nature of its business;

- collects information on the purpose and intended nature of the business relationship of a customer (natural or legal person);
- verifies the identity of the customer and the beneficial owner on the basis of documents, data or information obtained from reliable and independent sources;
- regular monitoring of customer's business relationship – transaction monitoring;
- continuous review and update of documents, data or information collected during the customer and beneficial owner identification process – ongoing due diligence.

2. when there is no possibility to fulfil the customer and beneficial owner identification requirements – suspension of transactions, refusal to establish or termination of business relationship;
3. applying customer and beneficial owner identification tools to existing customers;
4. suspension of a suspicious monetary operation or transaction;
5. reporting suspicious monetary operations or transactions;
6. a notice on virtual currency exchange operations or transactions in virtual currency where the value of such monetary operation or transaction is equal to or greater than EUR 15 000 or currency and virtual currency equivalent, whether the transaction is carried out in one or several interrelated transactions;
7. investigation of complex structure, unusually large and suspicious transactions;
8. information storage for a specified period of time;
9. designating staff responsible for implementing measures to prevent money laundering and / or terrorist financing;
10. staff training;
11. implementation of internal systems to enable prompt response to inquiries from the Financial Crime Investigation Service (FCIS) via secure channels and ensuring full confidentiality of inquiries;
12. confidentiality of the information provided to the FCIS;
13. setting internal policies, procedures and controls in place;
14. submission of information on the beneficial owners of the Depository Virtual Currency Wallet Operator and Virtual Currency Exchange Operator to the Legal Entities Participant Information System (JADIS) Manager.

4. BUSINESS WIDE ML / TF RISK ASSESSMENT

1. In the business wide ML / TF risk assessment (hereinafter – ML/TF risk assessment), the Company will analyze potential threats and vulnerabilities to money laundering and terrorist financing to which the business is exposed.
2. When identifying whether there is higher risk of money laundering and/or terrorist financing the Company will assess at least the following:

- **customer risk factors**:

a. the business relationship of the customer is conducted in unusual circumstances without any apparent economic or lawful purpose;

b. the customer is resident in a high risk third country;

c. legal persons or entities without legal person status acting as asset-holding vehicles;

d. legal entity has nominee shareholders or issued bearer shares;

e. the ownership structure of legal person appears unusual or excessively complex given the nature of the legal person's business;

The risk assessment requires that the Company knows its customers and the nature of their business. This is not limited to identification process or record keeping, but it is about understanding customers, including their activities, transaction patterns, and how they operate.

- product, service, transaction or delivery channel risk factors:

a. a product or transaction might favor anonymity;

b. business relationship 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;

e. transactions in oil, weapons, precious metals, tobacco products, cultural artefacts and other objects of archaeological, historical, cultural and religious significance or of rare scientific value, as well as in ivory and protected species.

The Company will identify products and services or combinations of them that may pose an elevated risk of money laundering or terrorist financing. Products and services that can support the movement and conversion of assets into, through and out of the financial system may pose a high risk.

- **geographical risk factors:**

  a. countries identified, on the basis of data of reports or similar documents by the Financial Action Task Force (FATF) or a similar regional organization, as having significant non-compliances with international requirements in their anti-money laundering and/or counter financing of terrorism systems;

  b. countries identified, on the basis of data by governmental and universally-recognized non-governmental organizations 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 organizations operating within their country.

Certain geographic locations potentially pose an elevated risk for money laundering and terrorist financing.

3. The ML / TF risk assessment results may identify increased-risk situations for which additional risk mitigation controls and monitoring may be required.

4. The ML / TF Risk assessment is a written document based on statistical data which outlines risk mitigation controls in place and their effectiveness so that residual risk can be assessed for each risk identified.

5. The results of the ML / TF risk assessment and remediation plan are communicated to Management Board who will need to approve remediation plan and assign responsible people to carry it out.

6. ML / TF risk assessment is carried out every year.

5. INTERNAL CONTROL PROCEDURES

1. The Company must set out AML/CFT internal controls covering:
    a. Roles and responsibilities over ML/TF prevention, including access to all information needed to perform daily duties according to roles and applicable laws;
    b. Risk assessment, risk controls
    c. Identification and verification of customer and beneficial owner;
    d. Sanctions and Politically Exposed People (PEP) screening;
    e. Ongoing due diligence;
    f. Transaction monitoring;
    g. Suspicious activity reports (SAR) to the Financial Crime Investigation Service (FCIS);
    h. Record keeping requirements;
    i. Management of information logs;
    j. Management Board information system to communicate internal and external information which might have impact to make decisions regarding ML/TF risk management.
    k. Constant employee training.
    l. Proper safeguarding of confidential information obtained while implementing AML/CTF program.
2. Internal controls in place and related procedures must be updated when:
    - European Commission completes supranational ML/TF risk assessment (announced here http://ec.europa.eu);
    - Lithuania completes national ML/TF risk assessment;
    - The FCIS orders to tighten internal control procedures;
    - There are significant changes in management structure and business nature;
    - Gaps are identified during periodical quality assurance process.

6. INTERNAL CONTROL PROCEDURES

1. Customers are classified with a risk level: low, medium, high risk and prohibited.
2. Customer risk scoring procedure and risk scoring matrix are provided in the On-boarding procedure.
3. When a customer is identified as high-risk, they are subject to appropriate enhanced due diligence measures.
4. For new customers risk scoring is performed before entering business relationship. The Company performs risk scoring for existing customers during ongoing due diligence.

7. IDENTIFICATION OF THE CUSTOMER AND THE BENEFICIAL OWNER

1. The Company will take measures to identify the customer and the beneficial owner as well as verify their identity:

   1.1. prior to establishing business relationship. The creation of a deposit wallet of virtual currencies is not a business relationship if no more than one transaction, operation, deposit or withdrawal has taken place in that wallet and the amount is less than EUR 1 000 or currency/ virtual currency equivalent;

   1.2. before:

   - executing occasional virtual currency exchange transactions or operations in virtual currency with funds equal to or above EUR 5,000 or currency/virtual currency equivalent.
   - occasional depositing or withdrawing of virtual currency amounting to or above EUR 5,000 or currency/virtual currency equivalent.
   - transaction is carried out in one or more interrelated transactions (the value of the virtual currency being determined at the time of the monetary transaction or operation) unless the customer and beneficial owner have already been identified.

   1.3. when there are doubts about the veracity or authenticity of the previously obtained identification data of the customer and the beneficial owner;

   1.4. in any other case when there are suspicions that an act of money laundering and/or terrorist financing is, was or will be carried out.

2. The Company will carry out customer's and beneficial owner's identification by applying a risk-based approach using:

   2.1. customer identification tools and customer due diligence (CDD) procedures;

   2.2. additional customer authentication tools and procedures for enhanced due diligence (EDD);

   2.3. simplified customer identification tools and procedures for simplified due diligence (SDD).

3. In case the Company is unable to meet the requirements set out in point 26.1., company will carry out the money laundering and/or terrorist financing threat assessment. After detecting the risk of money laundering and/or terrorist financing (ML/TF), the Company will report the suspicious monetary operation or transaction to the FCIS.

8. CUSTOMER DUE DILIGENCE

1. The purpose of customer due diligence (CDD) is to collect, process, verify and keep the information about the customers to minimize possible and/or potential ML/TF risks.
2. For all customers identification procedure must be completed prior entering relationship and it is necessary to complete the following steps:

   2.1. perform identification and verification – identify and verify the identity of the perspective customer and related parties;

   2.2. screen all customers and related parties against various EU, UN and OFAC Sanctions Lists;

   2.3. screen all customers and related parties to determine if the customer is a PEP or there are any PEP associated with the customer;

   2.4. verify as many customer details as possible in the public registers and perform open source search for all other relevant information.

   2.5. check the collected information;

   2.6. perform customer risk scoring.

3. When conducting identification procedure, collect natural person's identity document – passport, identity card or residence permit issued in the Republic of Lithuania which contains the following data:
    a. name/names;
    b. surname/surnames;
    c. 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);
    d. photograph;
    e. signature (except for the cases where it is optional in the identity document);
    f. citizenship (in the case of a stateless person – the state which issued the identity document).
4. When conducting identification procedure, collect legal entity's identity documents or copies thereof with a notarial certificate, confirming authenticity of the document's copy, which contain the following data:
    a. name;
    b. legal form, registered office/address, address of actual operation;
    c. registration number (if such number has been issued);
    d. an extract of registration and its date of issuance.
5. The identity of the legal person's representative shall be established in the same manner as the identity of the customer that is a natural person.
6. The customer must provide information about the legal person's director:
    a. name, surname;
    b. 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),
    c. citizenship (in the case of a stateless person – the state which issued the identity document).

9. SIMPLIFIED DUE DILIGENCE

1. Simplified due diligence (SDD) is the minimum level of due diligence that must be applied for a customer.
2. SDD may be carried out when financial institution assesses customer's risk as Low and one of the following conditions are fulfilled:
   a. Customer is a listed company (EU or equivalent).
   b. Customer is a government and municipality institution.
   c.
   d.
3. When applying SDD, Company must:
   - For individual customers – obtain name, surname and personal number.
   - For business customers – obtain name; legal form, registered office/address, address of actual operation; registration number (if such number has been issued).
   - Get customer's first top-up from his/her bank account in EU or third country having same level as Lithuanian AML requirements.
   - Ensure customer transaction monitoring.
   - Regularly check if customer is still eligible for SDD.
4. SDD is not permitted if there are mandatory conditions to perform EDD. Ensures effective communication of the importance of sanctions compliance throughout the organisation.

10. ENHANCED DUE DILIGENCE

1. Enhanced due diligence (EDD) refers to the situations where a customer presents higher risk of ML/TF and standard evidence of identity may be insufficient. Additional information needs to be obtained to assist with the customer approval and monitoring processes.

2. EDD involves objective, rigorous, and thorough research that provides a greater view of the customer's profile and the actions required to mitigate higher risks.
3. Enhanced due diligence (EDD) shall be conducted under the following circumstances:
    - when transactions or business relationships are conducted with politically exposed persons (PEP).
    - when business relationship is established with or transactions carried out with natural persons or legal entities from high-risk third countries identified by the European Commission.
    - when transactions or business relationships are conducted with natural persons or legal entities from countries identified by the Financial Task Force (FATF) as high risk.
    - when the Company assesses customer's risk as high using its risk scoring matrix.
4. When transactions or business relationships are conducted with PEPs, the Company must:
    - Have PEP procedure in place.
    - Obtain an approval from the senior manager to establish or continue business relationship with such costumers.
    - Identify and verify customer's source of wealth and (or) funds involved in a business relationship or transaction.
    - Carry out a constant enhanced monitoring of the business relationship with these customers.
5. When business relationship is established with or transactions carried out with natural persons or legal entities from high-risk third countries identified by the European Commission, the Company must:
    - obtain additional information about the customer and the beneficial owner.
    - obtain additional information on the intended nature of the business relationship.
    - obtain information on the source of wealth and (or) funds of the customer and beneficial owner.
    - obtain information on the reasons for anticipated or completed transactions.
    - obtain approval from senior management to establish or continue business relationship with these customers.
    - conduct enhanced ongoing monitoring of business relationships with these customers by increasing the number and timing of controls to be applied and selecting the types of transactions that will require further investigation.

- ensure that the first payment by a customer is made from that customer's bank account in European Union or in a third country which has equivalent AML requirements and supervision.

6. When transactions or business relationships are conducted with natural persons or legal entities from countries identified by the FATF as high risk OR the Company assesses customer's risk as high using its risk scoring matrix, the Company must:

   - Obtain senior management approval for establishing or continuing business relationships with these customers.
   - Identify and verify customer's source of wealth and (or) funds involved in a business relationship or transaction.
   - Conduct enhanced ongoing monitoring of business relationships with these customers.
   - Apply additional measures at the discretion of AML Officer:
     - ➢ obtain additional information about the customer and the beneficial owner.
     - ➢ obtain additional information on the intended nature of the business relationship.
     - ➢ obtain information on the source of wealth and (or) funds of the customer and beneficial owner.
     - ➢ obtain information on the reasons for anticipated or completed transactions.
     - ➢ ensure that the first payment by a customer is made from that customer's bank account in European Union or in a third country which has equivalent AML requirements and supervision.

11. ONGOING DUE DILIGENCE

1. Once a business relationship is established with a customer, the Company will monitor the business relationship to ensure that the transactions executed correspond to the information held by the Company about customer, his business, risk nature and source of funds. Further details are provided in the Ongoing Due Diligence (hereinafter – ODD) procedure.
2. The Company assesses each customer's risk score and assigns risk rate.
3. ODD means that documents, data or information collected during onboarding process is kept up-to-date and relevant by undertaking review of existing records. To have renewed KYC data is

fundamental to the monitoring and screening of the customer relationship and identifying unusual customer activity.

4. Risk rate of the customer determines how frequently the Company will review each business relationship and how frequently that business relationship information is updated. All customer relationships need ongoing due diligence, but high-risk customers will be monitored more frequently.

5. The scheduled frequency of review:

    - high-risk customers will be reviewed every six months,
    - medium risk customers will be reviewed annually, and
    - low-risk customers will be reviewed every two years.

6. ODD of each business relationship is intended to:

    - detect suspicious activity that must be reported;
    - keep customer KYC, the purpose and intended nature of the business relationship, and beneficial ownership information up to date;
    - re-assess the level of risk associated with the customer's transactions and activities;
    - determine whether the transactions or activities are consistent with the information previously obtained about the customer, including the risk scoring;
    - understand customer’s activities over time so that any changes can be measured to detect high risk.

7. These requirements do not need to follow the same timeframe, as long as high-risk customers are monitored more frequently and with more scrutiny than low-risk customers. Monitoring high-risk situations may include measures such as:

    - reviewing transactions based on an approved schedule that involves management sign-off;
    - developing reports or performing more frequent review of reports that list high-risk transactions, flagging activities or changes in activities from expectations and elevating concerns as necessary;
    - setting business limits or parameters regarding accounts or transactions that would trigger early warning signals and require mandatory review;
    - reviewing transactions more frequently against suspicious transaction indicators relevant to the relationship.

12. SANCTIONS AND POLITICALLY EXPOSED PEOPLE (PEP) SCREENING

1. The Republic of Lithuania follows the measures taken by the European Union, United Nations and the United States which are implemented through the Law on the Implementation of Economic and Other International Sanctions. These measures include a list of individuals and entities who/which are subject to sanctions. The Ministry of Foreign Affairs coordinates the implementation of international sanctions in Lithuania and provides information about it.
2. The Company must check if customers, representatives of the customers or the beneficial owners are not on the list of persons subject to international financial sanctions.
3. A check against sanctions lists shall be carried out during identification stage. All customers and suspicious customers will be continuously screened for sanctions for the length of the business relationship and at the time of transactions.
4. The Company will follow Instructions for the supervision of the appropriate administration of International Financial Sanctions in the field of Regulation of the Financial Crime Office under the Ministry of the Interior of the Republic of Lithuania approved by the FCIS Director on October 20th 2016 by Resolution No. V-273 "On the approval of the supervisory instructions in the field of regulation of the Financial Criminal Office of the Republic of Lithuania in the field of regulation on the implementation of international financial sanctions", therefore, the Company must:
    - provide information about the implementation of financial sanctions to the FCIS and the Ministry of Foreign Affairs of the Republic of Lithuania;
    - provide the FCIS with all data necessary for monitoring;
    - appoint employee(s) who would organize the implementation of financial sanctions, be in charge of termination of disposal of accounts, regular update of the list of entities which are under financial sanctions, reporting to the FCIS and other authorities responsible for monitoring of the implementation of international sanctions.
5. The Company will not establish business relationship with customers subject to international financial sanctions. For detailed process please refer to Onboarding procedure.
6. The Company must check if customers, representatives of the customers or the beneficial owners are not PEP.
7. A PEP self-declaration form is included in each KYC questionnaire and to verify information obtained from customer all names will be searched through credible sources of commercially or publicly available information.

8. PEP status itself does not incriminate individuals or entities. It does, however, put the customer or legal entity into a high-risk category and makes it subject to EDD.
9. Such customers remain high-risk for at least one year after officially seizing to be a PEP.
10. PEP screening is an ongoing process for All customers, placed under quarterly PEP screening process and suspicious customers will be continuous PEP screening process for the length of the business relationship

13. SUSPICIUOS MONETARY OPERATIONS OR TRANSACTIONS

1. Suspicious monetary operations or transactions shall be identified:
    - in accordance with the criteria for the identification of suspicious monetary transactions or transactions approved by Resolution No. V-240 of December 5th of 2014 of the Director of Financial Crime Investigation Service under the Ministry of Internal Affairs of the Republic of Lithuania "On the Approval of the List of Criteria for Money Laundering and Suspicious or Unusual Monetary Operations or Transactions Identification".
    - noting the activities of customers which, by their nature, may be related to money laundering and/or terrorist financing;
    - conducting customer’s and beneficial owner’s identification;
    - conducting ongoing monitoring of the customer's business relationship, including the investigation of transactions that have occurred during that relationship.
2. When suspicious monetary operation or transaction is detected, a documented investigation must be completed, that operation or transaction must be suspended, and a report made to the FCIS within three business hours. There is no minimal threshold or limit for such a report. Once suspicious monetary operation or transaction is reported to the FCIS then they are required to respond within ten working days. If the FCIS requests further information, then a response to that request must be provided immediately.
3. The Company shall notify the FCIS of the customer's identity data and information on the executed virtual currency exchange transactions (virtual currency purchase or sale in decree currency) or virtual currency transactions (virtual currency asset settlements) the value of a monetary operation or transaction is equal to or greater than EUR 15 000 or currency/virtual currency equivalent, whether the transaction is carried out in the context of one or more related monetary operations. The value of the virtual currency is determined at the time of the monetary operation or transaction.

4. In the event that a customer's monetary operation or transaction meets the requirements of both points 62 and 64 of this Policy, the Company shall submit notice of suspicious monetary operation or transaction and notification of executed virtual currencies exchange operation or transactions in virtual currency where the value of such monetary operation or transaction is equal to or greater than EUR 15 000 or currency/virtual currency equivalent, whether or not the transaction is executed in the context of one or more related monetary transactions to the 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 AML Officer in order not to accidentally disclose investigative actions to the customer.
6. Detailed process is described in the Transaction Monitoring procedure.

14. STORAGE OF INFORMATION AND DOCUMENTS

1. Accurate record keeping is imperative to evidence all financial crime risk management related activities and decisions as well as compliance with the AML. The Company must keep the following records:

   Customer Identification Records:

   - customer's identity documents and beneficial owner data;
   - all risk scoring records as well as the customer risk profile;
   - KYC questionnaire;
   - all records related to ODD.

   Transactions records:

   - a log containing transactional data during business relationship;
   - internal suspicious activity investigations;
   - a log of SAR reporting;
   - a log of virtual currency exchange transactions or transactions in virtual currency, if such monetary transaction or value of transaction is equal or greater than EUR 15 000 or currency/virtual currency equivalent, it is not important if transaction is executed through one or more related monetary transactions;

- a log of due to ML/TF reasons terminated business relationship.

Other records:

- evidence of the training programs on money laundering/terrorism financing prevention whether in-house or external;
- other records if required under the AML law of Lithuania as well as other legal acts related to the prevention of money laundering/terrorism financing;

2. The data in the registration logs must be entered in a chronological order, without delay, but not later than within 3 working days after the executions of the monetary operation or transaction.
3. All AML/CTF related records must be stored electronically, in a readily accessible and retrievable format and made available without delay upon request from the AML Officer or any relevant external bodies, including competent authorities. The Company will retain AML/CTF related records electronically.
4. Time period of record keeping:

1.	Log of Submitted SARs	To be kept for 8 years after terminating business relationship
2.	Log of virtual currency exchange and transactions equal or greater than EUR 15 000 or currency/virtual currency equivalent	
3.	Log of all customer transactions	
4.	Log of business relationships terminated due to ML/TF reasons	
5.	Copies of ID documents, identification information and KYC information	
6.	Digital currency wallet address together with owner's identity information	
7.	Correspondence with customer	To be kept for 5 years after terminating business relationship
8.	Supporting documents obtained from customer	To be kept for 8 years after completing transaction
9.	Internal investigation records of suspicious transactions	To be kept for 5 years

- All AML Officer reports to the General manager and the Board will be kept indefinitely.
- The Company maintains records of all AML training undertaken by staff, 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 Company.
- All SARs submitted including correspondence with the FCIS, the Bank of Lithuania (or any other government agency) will be kept for an unlimited period. Internal reports of suspicions will be kept for 10 (ten) years.

5. The time limits for record keeping may be extended additionally for no longer than two years upon a reasoned instruction of a competent authority.
6. The registration logs are kept in accordance to Resolution No. V-129 of September 4th of 2017 of the Director of Financial Crime Investigation Service under the Ministry of Internal Affairs of the Republic of Lithuania "On the Approval of the Rules for Keeping the Register of Suspicious or Unusual Monetary Operations and Transactions of the Customer and Identification of the Criteria that Characterizes Large-Scale Permanent and Regular Monetary Operations".

15. COMPLIANCE TRAINING

1. The Company has a yearly training program for all employees and other individuals who act on behalf of the Company to make sure that those who have contact with customers, who see customer transaction activity understands the reporting, customer identification and record keeping requirements.
2. All new employees of the Company are required to complete anti-money laundering and terrorist financing compliance training within their induction training period when they join the Company. All employees will be enrolled and undertake the comprehensive and regular Company-wide anti-money laundering and counter-terrorist financing training within their first six months of employment with the exception applicable to the employees who are directly involved in application of the AML/CTF measures (such as the AML Officer) who must be introduced to the procedures of the Company before they will start performing functions with the relation to AML/CTF.
3. The AML Officer 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. 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).

4. An employee log of assigned and completed training materials shall be kept up to date by the AML Officer and on file for five years (e.g. extract or download of training logs).
5. Relevant compliance training is for all employees and relevant outsourced service providers. This includes those persons in sales and in senior management and others who have responsibilities under the compliance regime, such as information technology officer and other staff responsible for designing and implementing electronic or manual internal controls. The AML Officer will review functions and arrange to provide suitable and customised training.
6. The Company's training will include at a minimum:
    - General background and history pertaining to money laundering controls, including the definitions of money laundering and terrorist financing, why criminals do it, and why stopping them is important.
    - Legal framework on what AML/CFT laws apply to institutions and their employees.
    - Penalties for AML/CFT violations, including criminal and civil penalties, fines, jail terms, as well as internal sanctions, such as disciplinary action up to and including termination of employment.
    - Internal policies, such as customer identification and verification procedures and policies, including Customer Due Diligence (CDD), Enhanced Due Diligence (EDD) and Ongoing Due Diligence (ODD).
    - Review of the internal AML/CFT and sanctions risk assessments.
    - Legal record keeping requirements.
    - Suspicious transaction monitoring and reporting requirements.
    - How to react when faced with a suspicious client or transaction.
    - How to respond to customers who want to circumvent reporting requirements.
    - Duties and accountability of employees.
    - Maintaining confidentiality with AML/CFT-related matters.
    - AML/CFT trends and emerging issues related to criminal activity, terrorist financing and regulatory requirements.
    - Money laundering schemes (preferably cases that have occurred at the company or at similar institutions), including how the pattern of activity was first detected, its impact on the institution, and its ultimate resolution.
7. Certain employees, such as those in compliance, 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.