ANTI-MONEY LAUNDERING AND COUNTER TERRORIST FINANCING COMPLIANCE POLICY

BeePay X UAB

Document History

Version	Approval Date	Author	Change Status	Approved by
1.0	2022-11-08	Ecovis Proventus Law	First issue	Italo Mainolfi

I. GENERAL PROVISIONS

1. BeePay X UAB (hereinafter – the Company) is a virtual currency exchange and virtual currency wallet 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 o

obligationsons.

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.

II. ROLES AND RESPONSIBILITIES

8. **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.

9. **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.

10. **The Compliance Officer (AML Officer)** is responsible for managing compliance risks, developing company's policies and procedures, and monitoring compliance issues. The AML Officer also a shareholder of the Company and a member of the board is responsible for reporting significant changes that may present high ML/TF risks to the Company. The AML Officer prepares monthly and quarterly reports for consideration to the General Manager and the Board and conducts risk assessments of compliance systems, develops regular random analysis. The AML Officer establishes and implements the risk scoring matrix following regulatory guidance and for review and approval by the General Manager.

11. **The MLR Officer (MLRO)** is responsible for Transaction monitoring, receiving internal disclosures and making reports to the Financial Crime Investigation Service (FCIS). First point of contact for all compliance issues from staff. MLRO undertakes regular random analysis of transactions including assessment of documentary evidence provided by Clients and prepares any necessary amendments to the Policy in line with risk assessment. MLRO ensures everyone is periodically informed of any changes in anti-money laundering and 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/CTF-related content for staff training programs. Independently from front office staff, MLRO reviews Client identification information to ensure that all the necessary information has been obtained.

12. **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.

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

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

12.1 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.

12.2 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;

12.3 applying customer and beneficial owner identification tools to existing customers;

12.4 suspension of a suspicious monetary operation or transaction;

12.5 reporting suspicious monetary operations or transactions;

12.6 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;

12.7 investigation of complex structure, unusually large and suspicious transactions;

12.8 information storage for a specified period of time;

12.9 designating staff responsible for implementing measures to prevent money laundering and / or terrorist financing;

12.10 staff training;

12.11 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;

12.12 confidentiality of the information provided to the FCIS;

12.13 setting internal policies, procedures and controls in place;

12.14 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.

IV. BUSINESS WIDE ML / TF RISK ASSESSMENT

13. Virtual currency carries a significant ML/TF risk, as there little to no prevention controls and measures at global level. In addition, virtual currency transactions may be anonymous and can allow individuals to purchase goods and services without possibility of identification. Supranational risk assessment report of EU considers the risk posed by virtual currency activities as significant. This leads to Company’s need to adapt it risk assessment procedures accordingly.

14. 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.

15. 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.

In addition to customer identification processes, the Company understands the ongoing problem with virtual currency anonymity both in Lithuanian jurisdiction, as well as abroad. Since the regulation and technological means to survey and control virtual currency trade are still being researched and implemented, the Company will closely follow official recommendations and guidelines issued by state authorities (such as Central bank of Lithuania).

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

a) virtual currency transactions are anonymous and usually completely untraceable;

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;

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 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.

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

16. 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.

17. 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.

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

V. INTERNAL CONTROL PROCEDURES

19. 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.

20. 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.

VI. CUSTOMER RISK SCORING

21. Customers are classified with a risk level: low, medium, high risk and prohibited.

22. Customer risk scoring procedure and risk scoring matrix are provided in the Onboarding procedure and have been performed automatically by our KYC provider based on our Risk Scoring program.

23. When a customer is identified as high-risk, they are subject to appropriate enhanced due diligence measures.

24. For new customers risk scoring is performed before entering business relationship. The Company performs risk scoring for existing customers during ongoing due diligence.

VII. IDENTIFICATION OF THE CUSTOMER AND THE BENEFICIAL OWNER

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

25.1. 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 700 or currency/ virtual currency equivalent;

25.2. before:

- executing occasional virtual currency exchange transactions or operations in virtual currency with funds equal to or above EUR 700 or currency/virtual currency equivalent.
- occasional depositing or withdrawing of virtual currency amounting to or above EUR 700 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.

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

25.4. 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.

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

1. customer identification tools and customer due diligence (CDD) procedures;
2. additional customer authentication tools and procedures for enhanced due diligence (EDD);
3. simplified customer identification tools and procedures for simplified due diligence (SDD).

27. The Company will not open anonymous accounts or accounts under obviously fictitious names and will not open accounts or otherwise start business relationships without requesting customer to provide data confirming his identity or if there is a reasonable suspicion that the provided data is fake or falsified.

28. 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.

VIII. CUSTOMER DUE DILIGENCE

28. 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.

29. For all customers identification procedure must be completed prior entering relationship and it is necessary to complete the following steps:

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

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

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

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

1.5. check the collected information;

1.6. perform customer risk scoring.

2. When conducting identification procedure, collect natural person's identity document – passport, identity card, driver's license (issued in the European Economic Area and complying with the requirements set out in Annex I of Directive 2006/126/EC of the European Parliament and of the Council of 20 December 2006 on driving licenses (Recast)) 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).

3. When the collected identity document does not contain the natural person's citizenship, the Company obtains information on the natural person's citizenship directly from official registers and in the absence of such records – from the customer.

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).

IX. SIMPLIFIED DUE DILIGENCE

7. Simplified due diligence (SDD) is the minimum level of due diligence that must be applied for a customer.

8. SDD may be carried out when the Company 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.

9. 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, payment or electronic money 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.

10. SDD is not permitted if there are mandatory conditions to perform EDD or CDD.

X. ENHANCED DUE DILIGENCE

39. 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.

40. 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.

41. 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 Action Task Force (FATF) as high risk.
- when the Company assesses customer's risk as high using its risk scoring matrix.

42. 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.

43. 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, payment or electronic money account in European Union or in a third country which has equivalent AML requirements and supervision.

44. 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 reasons for anticipated or completed transactions.
  - ➢ ensure that the first payment by a customer is made from that customer's bank, payment or electronic money account in European Union or in a third country which has equivalent AML requirements and supervision.

XI. ONGOING DUE DILIGENCE

45. 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.

46. The Company assesses each customer's risk score and assigns risk rate.

47. 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.

48. 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.

49. 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.

50. 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.

51. 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.

XII. SANCTIONS AND POLITICALLY EXPOSED PEOPLE (PEP) SCREENING

52. 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.

53. 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.

54. A check against sanctions lists shall be carried out during the identification stage. All customers are continuously screened for sanctions for the length of the business relationship and at the time of transactions.

55. 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.

56. The Company will not establish business relationship with customers subject to international financial sanctions. For detailed process please refer to Onboarding procedure.

57. The Company must check if customers, representatives of the customers or the beneficial owners are not PEP.

58. 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.

59. 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.

60. Such customers remain high-risk for at least one year after officially seizing to be a PEP.

61. PEP screening is an ongoing process for all customers for the length of the business relationship.

XIII. SUSPICIUOS MONETARY OPERATIONS OR TRANSACTIONS

62. 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.

63. 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 after suspicious activity determination. There is no minimal threshold or limit for such a report. Once suspicious monetary operation or transaction is reported to the FCIS, 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.

64. 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.

65. 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.

66. 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.

67. Detailed process is described in the Transaction Monitoring procedure.

XIV. STORAGE OF INFORMATION AND DOCUMENTS

68. 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;

69. 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.

1. 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.

2. 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
10.	Training log and related documents	To be kept for 5 years after the end of training

- 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.

72. The time limits for record keeping may be extended additionally for no longer than two years upon a reasoned instruction of a competent authority.

73. 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".

XV. COMPLIANCE TRAINING

74. 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.

75. 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.

76. 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).

77. 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).

78. 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 customized training.

79. 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.

80. 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.

KOVOS SU PINIGŲ PLOVIMU IR TERORISTŲ FINANSAVIMU ATITIKTIES POLITIKA

BeePay X UAB

Dokumento istorija

Versija	Patvirtinimo data	Sudarė	Pakeitimai	Patvirtino
1.0	2022-08-11		Pirmasis leidimas	

I. BENDROSIOS NUOSTATOS

1. BeePay X UAB (toliau – Bendrovė) yra virtualios valiutos keitimo ir virtualios valiutos piniginės bendrovė, veikianti pagal Lietuvos Respublikos įstatymus. Bendrovė yra įsipareigojusi vykdyti veiklą skaidriai ir atvirai, laikantis savo reguliavimo įsipareigojimų.

2. Šia politika įgyvendinamas 1997 m. birželio 19 d. Lietuvos Respublikos Pinigų plovimo ir teroristų finansavimo prevencijos įstatymas Nr. VIII-275 Nr. XIII-2584 (toliau – Įstatymas).

3. Įgyvendindama pinigų plovimo ir (arba) teroristų finansavimo prevencijos priemones, Bendrovė vadovaujasi šiais pagrindiniais Finansinių nusikaltimų tyrimo tarnybos direktoriaus išduotais dokumentais:

- Techniniais reikalavimais kliento tapatybės nustatymo procesui, kai tapatybė nustatoma nuotoliniu būdu, naudojantis elektroninėmis priemonėmis, leidžiančiomis tiesioginio vaizdo perdavimą, patvirtintais Finansinių nusikaltimų tyrimo tarnybos prie Lietuvos Respublikos Vidaus reikalų ministerijos direktoriaus 2016 m. lapkričio 30 d. sprendimu Nr. V-314 „Dėl techninių reikalavimų kliento tapatybės nustatymo procesui, kai tapatybė nustatoma nuotoliniu būdu, naudojantis elektroninėmis priemonėmis, leidžiančiomis tiesioginio vaizdo perdavimą“ (toliau – Techniniai reikalavimai).
- Finansinių nusikaltimų tyrimo tarnybos prie Lietuvos Respublikos Vidaus reikalų ministerijos direktoriaus 2014 m. gruodžio 5 d. sprendimu Nr. V-240 „Dėl galimo pinigų plovimo ir įtartinų piniginių operacijų ar sandorių atpažinimo kriterijų sąrašo patvirtinimo“.
- Finansinių nusikaltimų tyrimo tarnybos prie Lietuvos Respublikos Vidaus reikalų ministerijos direktoriaus 2020 m. sausio 5 10 d. sprendimu Nr. V- „Dėl depozitinių virtualiųjų valiutų piniginių operatoriams ir virtualiųjų valiutų keityklos operatoriams skirtų nurodymų, kuriais siekiama užkirsti kelią pinigų plovimui ir (ar) teroristų finansavimui, patvirtinimo“.
- Finansinių nusikaltimų tyrimo tarnybos prie Lietuvos Respublikos Vidaus reikalų ministerijos direktoriaus 2016 m. spalio 20 d. sprendimu Nr. V-273 „Dėl tinkamo tarptautinių finansinių sankcijų įgyvendinimo finansinių nusikaltimų tyrimo tarnybos prie Lietuvos Respublikos Vidaus reikalų ministerijos reguliavimo srityje priežiūros nurodymų patvirtinimo“.

4. Priežiūros institucijos turi teisę savo iniciatyva pradėti įstatyme nustatytų pinigų plovimo ir (arba) teroristų finansavimo prevencijos priemonių įgyvendinimo patikrinimus, remiantis priežiūros institucijų patikrinimo planu (priežiūros planu).

4. Taip pat priežiūros institucijos gali pradėti patikrinimus, susijusius su galimais Įstatymo pažeidimais, jei gavo pranešimą ar bet kokius kitus duomenis, kuriuose užfiksuotos galimų Įstatymo pažeidimų aplinkybės.

5. Šiurkščiu Įstatymo pažeidimu laikoma:

- reikalavimų dėl išsamaus kliento patikrinimo nesilaikymas;
- reikalavimų dėl pranešimų apie įtartinas pinigų, virtualios valiutos keitimo operacijas ar sandorius virtualia valiuta pateikimo nesilaikymas;
- reikalavimų dėl informacijos saugojimo nesilaikymas;
- kai įpareigotasis subjektas neįvedė vidaus kontrolės procedūrų.

7. Šioje Politikoje naudojamos sąvokos yra apibrėžtos Įstatyme.

II. VAIDMENYS IR ATSAKOMYBĖS

8. **Valdyba** atlieka labai svarbų priežiūros vaidmenį - būdama aukščiausiąja bendrovės vadovybe, ji turėtų patvirtinti ir prižiūrėti rizikos, rizikos valdymo ir atitikties politiką. Valdyba taip pat turėtų aiškiai suprasti PP riziką, įskaitant laiku pateiktą, išsamią ir tikslią informaciją, susijusią su rizikos vertinimu, kad galėtų priimti pagrįstus sprendimus. Kartu su Generaliniu direktoriumi Valdyba turėtų paskirti kvalifikuotą kovos su PP pareigūną, kuris būtų visiškai atsakingas už kovos su PP funkciją, ir suteikti šiam aukšto lygio pareigūnui pakankamai įgaliojimų tam, kad iškėlus klausimus jiems būtų skiriamas tinkamas Valdybos, Generalinio direktoriaus ir vadovų dėmesys. Valdyba yra atsakinga už bendrą Bendrovės kovos su PP / TF politiką ir užtikrina, kad būtų skiriama pakankamai išteklių tinkamam darbuotojų mokymui ir rizikos sistemų diegimui. Valdyba gaus ir apsvarstys Kovos su PP pareigūno pateiktas ketvirčio atitikties ataskaitas.

6. **Generalinis direktorius** gaus ir apsvarstys kovos su PP pareigūno atsiųstas mėnesines atitikties ataskaitas ir, jei reikia, įgalios atlikti pakeitimus pagal rekomendacijas. Generalinis direktorius taip pat gaus ataskaitas apie ypač reikšmingus pokyčius, kurie gali kelti pavojų organizacijai. Rengiant kovos su PP programą, Kovos su PP pareigūnui gali būti teikiama pagalba.

7. **Atitikties pareigūnas** (Kovos su PP pareigūnas) yra atsakingas už atitikties rizikos valdymą, įmonės politikos ir procedūrų kūrimą bei atitikties problemų stebėjimą. Kovos su PP pareigūnas yra atsakingas už pranešimų apie reikšmingus pokyčius, kurie gali sukelti didelę PP / TF riziką Bendrovei, pateikimą. Kovos su PP pareigūnas rengia mėnesines ir ketvirčio ataskaitas Generaliniam direktoriui ir Valdybai, atlieka atitikties sistemų rizikos vertinimą, rengia reguliarią atsitiktinę analizę. Vadovaudamasis reguliavimo gairėmis, Kovos su PP pareigūnas nustato ir įgyvendina rizikos vertinimo formą bei teikia Generaliniam direktoriui peržiūrėti bei patvirtinti.

8. **PP ataskaitų teikimo pareigūnas (PPATP)** yra atsakingas už sandorių stebėjimą, vidinės informacijos gavimą ir ataskaitų teikimą Finansinių nusikaltimų tyrimo tarnybai (FNTT). Pirmasis kontaktinis asmuo visais su atitiktimi susijusiais klausimais iš darbuotojų.

PPATP įsipareigoja reguliariai atlikti atsitiktinę sandorių analizę, įskaitant Klientų pateikiamų dokumentinių įrodymų vertinimą, bei reikalingus šios Politikos pakeitimus, atsižvelgiant į rizikos vertinimą. PPATP užtikrina, kad visi būtų periodiškai informuojami apie bet kokius kovos su pinigų plovimu ir teroristų finansavimu teisės aktų, politikos ir procedūrų pakeitimus, taip pat apie dabartinius pokyčius ir pinigų plovimo ar teroristų veiklos finansavimo schemų pokyčius, susijusius su jų darbo vieta, kuriant su kova su pinigų plovimu ir teroristų finansavimu susijusį darbuotojams skirtų mokymo programų turinį. Nepriklausomai nuo su klientais bendraujančių darbuotojų, PPATP peržiūri Kliento tapatybės nustatymo informaciją siekiant užtikrinti, kad buvo gauta visa reikalinga informacija.

9. **Kiti darbuotojai** yra atsakingi už tai, kad susipažintų su šia Politika, kitomis vidaus procedūromis, susijusiomis su jų pagrindiniu vaidmeniu ir atsakomybių supratimu. Užtikrina, kad būtų laikomasi kovos su PP / TF procedūrų. Užtikrina, kad apie bet kokią įtartiną veiklą būtų pranešta Kovos su PP pareigūnui.

III. PRIEMONĖS, SKIRTOS UŽKIRSTI KELIĄ PINIGŲ PLOVIMUI IR (ARBA) TERORISTŲ FINANSAVIMUI

12. Bendrovė įgyvendina šias priemones, skirtas užkirsti kelią pinigų plovimui ir (arba) teroristų finansavimui:

12.1 Kliento ir naudos gavėjo tapatybės nustatymas:

- nustatoma, ar klientas veikia savo vardu ar yra kontroliuojamas;
- jei klientas veikia per atstovą, nurodomas kliento atstovas;
- nustatoma kliento (fizinio asmens) tapatybė;
- nustatoma kliento (juridinio asmens) tapatybė;
- nustatoma kliento (juridinio asmens) naudos gavėjo tapatybė;
- renkama informacija apie kliento (juridinio asmens) direktorių;
- renkama informacija apie kliento juridinio asmens nuosavybės ir valdymo struktūrą, jo verslo pobūdį;
- renkama informacija apie kliento (fizinio ar juridinio asmens) dalykinių santykių tikslą ir numatytą pobūdį;
- tvirtinama kliento ir naudos gavėjo tapatybė, remiantis dokumentais, duomenimis ar informacija, gauta iš patikimų ir nepriklausomų šaltinių;
- reguliariai stebimi kliento dalykiniai santykiai – sandorių stebėsena;
- nuolat peržiūrimi ir atnaujinami kliento ir naudos gavėjo tapatybės nustatymo proceso metu surinkti dokumentai, duomenys ar informacija – nuolatinis išsamus patikrinimas.

12.2 kai nėra galimybės įvykdyti kliento ir naudos gavėjo tapatybės nustatymo reikalavimų – sandorių sustabdymas, atsisakymas užmegzti dalykinius santykius ar jų nutraukimas;

12.3 klientų ir naudos gavėjų tapatybės nustatymo priemonių taikymas esamiems klientams;

12.4 įtartinos piniginės operacijos ar sandorio sustabdymas;

12.5 pranešimas apie įtartinas pinigines operacijas ar sandorius;

12.6 pranešimas apie virtualios valiutos keitimo operacijas arba sandorius virtualia valiuta, kai tokios piniginės operacijos ar sandorio vertė yra lygi arba didesnė nei 15 000 EUR arba ją atitinkanti suma valiuta ir virtualiąja valiuta, nesvarbu, ar sandoris vykdomas vienu ar keliais tarpusavyje susijusiais sandoriais;

12.7 sudėtingos struktūros, neįprastai didelių ir įtartinų sandorių tyrimas;

12.8 informacijos saugojimas nurodytą laiką;

12.9 darbuotojų, atsakingų už priemonių, skirtų užkirsti kelią pinigų plovimui ir (arba) teroristų finansavimui, paskyrimas;

12.10 darbuotojų mokymai;

12.11 vidaus sistemų diegimas, kad būtų galima greitai reaguoti į Finansinių nusikaltimų tyrimo tarnybos (FNTT) užklausas saugiais kanalais ir užtikrinti visišką užklausų konfidencialumą;

12.12 FNTT pateiktos informacijos konfidencialumas;

12.13 vidaus politikų, procedūrų ir kontrolės priemonių nustatymas;

12.14 informacijos apie faktinius Depozitinės virtualiosios valiutos piniginės operatoriaus ir Virtualiosios valiutos keityklos operatoriaus savininkus pateikimas Juridinių asmenų dalyvių informacinės sistemos (JADIS) valdytojui.

IV. VISO VERSLO PP / TF RIZIKOS VERTINIMAS

13. Virtualioji valiuta kelia didelę PP / TF riziką, nes prevencijos kontrolės ir priemonių pasauliniu lygmeniu beveik nėra. Be to, sandoriai virtualiąja valiuta paprastai yra anoniminiai ir asmenys gali pirkti prekes bei paslaugas be galimybės nustatyti jų tapatybę. Tarptautinėje ES rizikos vertinimo ataskaitoje rizika, kurią kelia virtualiosios valiutos veikla, laikoma didele. Todėl Bendrovė turi atitinkamai pritaikyti rizikos vertinimo procedūras.

14. Viso verslo PP / TF rizikos vertinime (toliau – PP / TF rizikos vertinimas) Bendrovė analizuos galimas pinigų plovimo ir teroristų finansavimo grėsmes ir pažeidžiamumą, su kuriuo susiduria verslas.

10. Nustatant, ar yra didesnė pinigų plovimo ir (arba) teroristų finansavimo rizika, Bendrovė įvertins bent šiuos dalykus:

- **kliento rizikos požymius:**

a) kliento dalykiniai santykiai vykdomi neįprastomis aplinkybėmis be akivaizdaus ekonominio ar teisėto tikslo;

b) klientas reziduoja didelės rizikos trečiojoje šalyje;

c) juridiniai asmenys ar juridinio asmens statuso neturintys subjektai vykdo asmeninės turto valdymo įmonės veiklą;

d) juridinis asmuo turi formalių akcininkų arba išleistų pareikštinių akcijų;

e) juridinio asmens nuosavybės struktūra atrodo neįprasta ar pernelyg sudėtinga, atsižvelgiant į juridinio asmens verslo pobūdį;

Rizikos vertinimui reikia, kad Bendrovė žinotų savo klientus ir jų verslo pobūdį. Tai neapsiriboja tapatybės nustatymo procesu ar įrašų saugojimu; svarbu suprasti klientus, įskaitant jų veiklą, sandorių modelius ir jų veikimą.

Be klientų tapatybės nustatymo procesų, Bendrovė supranta nuolatinę virtualiosios valiutos anonimiškumo problemą tiek Lietuvos jurisdikcijoje, tiek užsienyje. Kadangi reguliavimas ir technologinės priemonės, skirtos prižiūrėti ir kontroliuoti prekybą virtualiąja valiuta, vis dar tiriamos ir įgyvendinamos, Bendrovė atidžiai laikysis oficialių valstybės institucijų (pvz., Lietuvos centrinio banko) rekomendacijų ir nurodymų.

· **produkto, paslaugos, sandorio ar paslaugų teikimo kanalo rizikos požymius:**

a) sandoriai virtualiąja valiuta yra anoniminiai ir dažniausiai visiškai neatsekami;

b) dalykiniai santykiai ar sandoriai užmezgami arba vykdomi fiziškai nedalyvaujant;

c) mokėjimai gaunami iš nežinomų ar nesusijusių trečiųjų šalių;

d) produktai ir verslo praktika, įskaitant paslaugų teikimo mechanizmą, yra nauja ir naujos ar vystomos technologijos naudojamos tiek naujiems, tiek esamiems produktams;

Bendrovė nustatys produktus ir paslaugas ar jų derinius, kurie gali kelti didesnę pinigų plovimo ar teroristų finansavimo riziką. Produktai ir paslaugos, kurios gali padėti perkelti ir konvertuoti turtą į finansų sistemą, per ją ir iš jos, kelia didelę riziką.

· **teritorijos rizikos požymiai:**

a) remiantis Finansinių veiksmų darbo grupės (FATF) ar panašios regioninės organizacijos ataskaitų ar panašių dokumentų duomenimis, valstybėje nustatyta reikšmingų kovos su pinigų plovimu ir teroristų finansavimu sistemos neatitikčių tarptautiniams reikalavimams;

b) remiantis vyriausybinių ir visuotinai pripažintų nevyriausybinių organizacijų, stebinčių ir vertinančių korupcijos lygį, duomenimis, valstybėje nustatytas didelis korupcijos ar kitos nusikalstamos veiklos lygis;

c) valstybei taikomos sankcijos, embargas ar panašios priemonės, paskelbtos, pavyzdžiui, Europos Sąjungos arba Jungtinių Tautų;

d) valstybė finansuoja arba remia teroristų veiklą arba valstybių teritorijoje veikia į sąrašus įtrauktos teroristų organizacijos.

Tam tikros geografinės vietovės gali kelti didesnę pinigų plovimo ir teroristų finansavimo riziką.

15. PP / TF rizikos vertinimo rezultatais gali būti nustatytos padidintos rizikos situacijos, kurioms gali prireikti papildomų rizikos mažinimo kontrolės priemonių ir stebėsenos.

11. PP / TF rizikos vertinimas yra rašytinis dokumentas, pagrįstas statistiniais duomenimis, kuriame išdėstytos esamos rizikos mažinimo kontrolės priemonės ir jų veiksmingumas tam, kad būtų galima įvertinti kiekvienos nustatytos rizikos likutinę riziką.

12. PP / TF rizikos vertinimo ir ištaisymo plano rezultatai perduodami Valdybai, kuri turės patvirtinti ištaisymo planą ir paskirti žmones, atsakingus už jo įgyvendinimą.

13. PP / TF rizikos vertinimas atliekamas kiekvienais metais.

V. VIDAUS KONTROLĖS PROCEDŪROS

19. Bendrovė turi nustatyti kovos su PP / TF vidaus kontrolę, apimančią:

- **a.** Vaidmenis ir atsakomybes už PP / TF prevenciją, įskaitant prieigą prie visos informacijos, reikalingos kasdienėms pareigoms atlikti pagal vaidmenis ir taikomus įstatymus;
- **b.** Rizikos vertinimą, rizikos kontrolės priemones
- **c.** Kliento ir naudos gavėjo tapatybės nustatymą ir patvirtinimą;
- **d.** Sankcijų ir politiškai pažeidžiamų (paveikiamų) asmenų (*angl. Politically Exposed People*, toliau - PPA) patikrinimą;
- **e.** Nuolatinį išsamų patikrinimą;
- **f.** Sandorių stebėjimą;
- **g.** Pranešimus apie įtartiną veiklą (*angl, Suspicious Activity Report*, toliau - PĮV) Finansinių nusikaltimų tyrimo tarnybai (FNTT);
- **h.** Įrašų tvarkymo reikalavimus;
- **i.** Informacijos žurnalų valdymą;
- **j.** Valdybos informacinę sistemą, skirtą perduoti vidinę ir išorinę informaciją, kuri gali turėti įtakos priimant sprendimus dėl PP / TF rizikos valdymo.
- **k.** Nuolatinius darbuotojų mokymus.
- **l.** Tinkamą konfidencialios informacijos, gautos įgyvendinant kovos su PP / TF programą, apsaugą.

20. Įdiegta vidaus kontrolė ir susijusios procedūros turi būti atnaujintos, kai:

- Europos Komisija atlieka tarptautinį PP / TF rizikos vertinimą (paskelbta čia http://ec.europa.eu);
- Lietuva atlieka nacionalinį PP / TF rizikos vertinimą;
- FNTT nurodo sugriežtinti vidaus kontrolės procedūras;
- Yra didelių valdymo struktūros ir veiklos pobūdžio pakeitimų;
- Periodinio kokybės užtikrinimo proceso metu nustatomos spragos.

VI. KLIENTO RIZIKOS VERTINIMAS

21. Klientai klasifikuojami pagal rizikos lygį: mažos, vidutinės, didelės rizikos ir draudžiami.

14. Kliento rizikos vertinimo procedūra ir rizikos vertinimo forma pateikiamos Priėmimo procedūroje.

15. Kai nustatoma, kad klientas yra didelės rizikos, jam taikomos atitinkamos griežtesnės išsamaus patikrinimo priemonės.

16. Naujų klientų atveju, rizikos vertinimas atliekamas prieš užmezgant dalykinius santykius. Bendrovė atlieka esamų klientų rizikos vertinimą nuolatinio išsamaus patikrinimo metu.

VII. KLIENTO IR NAUDOS GAVĖJO TAPATYBĖS NUSTATYMAS

25. Bendrovė imsis priemonių siekiant nustatyti ir patvirtinti kliento ir naudos gavėjo tapatybę:

16.1. prieš užmezgant dalykinius santykius. Depozitinės virtualiųjų valiutų piniginės sukūrimas nėra dalykiniai santykiai, jei toje piniginėje buvo atliktas ne daugiau kaip vienas sandoris, operacija, indėlis ar išėmimas ir suma yra mažesnė nei 1 000 EUR arba ją atitinkanti suma valiuta / virtualiąja valiuta;

16.2. prieš:

- retkarčiais atliekant virtualiosios valiutos keitimo sandorius ar operacijas virtualiąja valiuta, kai lėšos yra ne mažesnės kaip 1 000 EUR arba ją atitinkanti suma valiuta / virtualiąja valiuta.
- retkarčiais įnešant ar atsiimant virtualiąją valiutą, kurios suma yra 1 000 EUR arba didesnė, arba ją atitinkanti suma valiuta / virtualiąja valiuta.

- sandoris atliekamas vienu ar daugiau tarpusavyje susijusių sandorių (virtualiosios valiutos vertė nustatoma piniginio sandorio ar operacijos metu), nebent kliento ir naudos gavėjo tapatybė jau buvo nustatyta.

16.3. kai kyla abejonių dėl anksčiau gautų kliento ir naudos gavėjo tapatybės nustatymo duomenų tikrumo ar autentiškumo;

16.4. bet kuriuo kitu atveju, kai kyla įtarimas, kad yra, buvo ar bus vykdoma pinigų plovimo ir (ar) teroristų finansavimo veika.

26. Bendrovė nustatys kliento ir naudos gavėjo tapatybę, taikydama rizika pagrįstą metodą, naudojant:

1. klientų tapatybės nustatymo priemones ir klientų išsamaus patikrinimo (*angl. Customer Due Diligence*, toliau - KIP) procedūras;
2. papildomas klientų autentifikavimo priemones ir procedūras, skirtas griežtesniam išsamiam patikrinimui (*angl. Enhanced Due Diligence*, toliau - GIP);
3. supaprastintas klientų tapatybės nustatymo priemones ir supaprastinto išsamaus patikrinimo (*angl. Simplified Due Diligence*, toliau - SIP) procedūras.

27. Bendrovė neatidarys anoniminių sąskaitų ar sąskaitų akivaidžiai fiktyviais vardais, taip pat neatidarys sąskaitų ar kitaip nepradės dalykinių santykių nepareikalavus kliento tapatybę patvirtinančių duomenų arba kilus pagrįstam įtarimui, kad šiuose dokumentuose įrašyti duomenys yra netikri ar suklastoti.

28. Jei Bendrovė negali įvykdyti 26.1 punkte nustatytų reikalavimų, Bendrovė atliks pinigų plovimo ir (arba) teroristų finansavimo grėsmės vertinimą. Nustačiusi pinigų plovimo ir (arba) teroristų finansavimo (PP / TF) riziką, Bendrovė praneš apie įtartiną piniginę operaciją ar sandorį FNTT.

VIII. KLIENTO IŠSAMUS PATIKRINIMAS

28. Klientų išsamaus patikrinimo (*angl. Customer Due Diligence*, toliau - KIP) tikslas yra rinkti, tvarkyti, patvirtinti ir saugoti informaciją apie klientus siekiant sumažinti galimą ir (arba) potencialią PP / TF riziką.

17. Visų klientų nustatymo procedūra turi būti atlikta prieš pradedant santykius ir būtina atlikti šiuos veiksmus:

10.1. atlikti tapatybės nustatymą ir patvirtinimą - nustatyti ir patvirtinti galimo kliento ir susijusių šalių tapatybę;

10.2. tikrinti visus klientus ir susijusias šalis įvairiuose ES, JT ir OFAC sankcijų sąrašuose;

10.3. tikrinti visus klientus ir susijusias šalis siekiant nustatyti, ar klientas yra PPA, ar su klientu susijęs PPA;

10.4. patikrinti kuo daugiau klientų duomenų viešuosiuose registruose ir atlikti visos kitos svarbios informacijos atvirojo kodo paiešką.

10.5. patikrinti surinktą informaciją;

10.6. atlikti kliento rizikos vertinimą.

18. Atlikdami tapatybės nustatymo procedūrą, gaukite fizinio asmens tapatybės dokumentą – pasą, asmens tapatybės kortelę, vairuotojo pažymėjimą (išduotą Europos ekonominėje erdvėje ir atitinkantį 2006 m. gruodžio 20 d. Europos Parlamento ir Tarybos direktyvos 2006/126/EB I priede nustatytus reikalavimus dėl vairuotojo pažymėjimų (nauja redakcija)) arba Lietuvos Respublikoje išduotą leidimą gyventi, kuriuose yra šie duomenys:

a. vardas / vardai;
b. pavardė / pavardės;
c. asmens kodas (užsieniečiui – gimimo data (jei yra – asmens kodas ar bet kuri kita tam asmeniui suteikta unikali simbolių seka, skirta asmens tapatybei nustatyti), leidimo gyventi Lietuvos Respublikoje numeris ir galiojimo laikas ir jo išdavimo vieta ir data (taikoma užsieniečiams);
d. nuotrauka;
e. parašas (išskyrus atvejus, kai asmens tapatybės dokumente tai neprivaloma);
f. pilietybė (asmens be pilietybės atveju – tapatybę patvirtinantį dokumentą išdavusi valstybė).

19. Kai gautame asmens tapatybės dokumente nėra fizinio asmens pilietybės, Bendrovė informaciją apie fizinio asmens pilietybę gauna tiesiogiai iš oficialių registrų, o jei tokių įrašų nėra – iš kliento.

20. Atlikdami tapatybės nustatymo procedūrą, gaukite juridinio asmens tapatybę patvirtinančius dokumentus arba jų kopijas su notaro liudijimu, patvirtinančiu dokumento kopijos tikrumą, kuriuose yra šie duomenys:

a. pavadinimas:
b. teisinė forma, buveinė / adresas, faktinės veiklos vykdymo adresas;
c. kodas (jeigu toks kodas yra suteiktas);
d. registracijos išrašas ir jo išdavimo data.

21. Juridinio asmens atstovo tapatybė nustatoma taip pat, kaip ir kliento – fizinio asmens tapatybė.

22. Klientas turi pateikti informaciją apie juridinio asmens direktorių:

a. vardas, pavardė;

b. asmens kodas (užsieniečiui – gimimo data (jei yra – asmens kodas ar bet kuri kita tam asmeniui suteikta unikali simbolių seka, skirta asmens tapatybei nustatyti),
c. pilietybė (asmens be pilietybės atveju – tapatybę patvirtinantį dokumentą išdavusi valstybė).

IX. SUPAPRASTINTAS IŠSAMUS PATIKRINIMAS

23. Supaprastintas išsamus patikrinimas (SIP) yra minimalus išsamaus patikrinimo lygis, kuris turi būti taikomas klientui.

24. SIP gali būti atliekamas, kai finansų įstaiga įvertina kliento riziką kaip mažą ir yra įvykdyta viena iš šių sąlygų:

a. Klientas yra į sąrašus įtraukta bendrovė (ES ar lygiaverčius).
b. Klientas yra vyriausybės ir savivaldybės institucija.

25. Taikant SIP Bendrovė privalo:

- Individualiems klientams – gauti vardą, pavardę ir asmens kodą.
- Verslo klientams – gauti pavadinimą, teisinę formą, buveinę / adresą, faktinės veiklos vykdymo adresą; įmonės kodą (jeigu toks kodas yra suteiktas).
- Gauti pirmąjį kliento papildymą iš jo banko sąskaitos, mokėjimo ar elektorninių pinigų sąskaitos ES ar trečiojoje šalyje, kurios lygis atitinka Lietuvos kovos su pinigų plovimu reikalavimus.
- Užtikrinti kliento sandorių stebėseną.
- Reguliariai tikrinti, ar klientas vis dar atitinka SIP.

26. SIP negalima atlikti, jei yra sąlygos, kurioms esant privaloma atlikti GIP ar KIP.

X. GRIEŽTESNIS IŠSAMUS PATIKRINIMAS

39. Griežtesnis išsamus patikrinimas (GIP) taikomas situacijoms, kai klientas turi didesnę PP / TF riziką, o įprastų tapatybės įrodymų gali nepakakti. Siekiant pagreitinti klientų patvirtinimo ir stebėjimo procesus, reikia gauti papildomos informacijos.

27. GIP apima objektyvius, griežtus ir išsamius tyrimus, kurie suteikia daugiau informacijos apie kliento profilį ir veiksmus, kurių reikia norint sumažinti didesnę riziką.

28. Griežtesnis išsamus patikrinimas (GIP) atliekamas esant tokioms aplinkybėms:

- kai sandoriai ar dalykiniai santykiai vykdomi su politiškai pažeidžiamais (paveikiamais) asmenimis (PPA).
- kai dalykiniai santykiai kuriami ar sandoriai atliekami su Europos Komisijos nustatytose didelės rizikos trečiosiose valstybėse gyvenančiais fiziniais asmenimis ar ten įsteigtais juridiniais asmenimis.

- kai sandoriai ar dalykiniai santykiai vykdomi su fiziniais ar juridiniais asmenimis iš valstybių, kurias Finansinių veiksmų darbo grupė (FATF) nustatė kaip didelės rizikos valstybes.
- kai Bendrovė vertina kliento riziką kaip didelę naudodama savo rizikos vertinimo formą.

42. Kai sandoriai ar dalykiniai santykiai vykdomi su PPA, Bendrovė privalo:

- Taikyti PPA procedūrą.
- Gauti vyresniojo vadovo patvirtinimą norint užmegzti ar tęsti dalykinius santykius su tokiais klientais.
- Nustatyti ir patvirtinti kliento turto ir (arba) lėšų šaltinį, susijusį su dalykiniais santykiais ar sandoriu.
- Nuolat stiprinti dalykinių santykių su šiais klientais stebėseną.

43. Kai dalykiniai santykiai kuriami ar sandoriai atliekami su Europos Komisijos nustatytose didelės rizikos trečiosiose valstybėse gyvenančiais fiziniais asmenimis ar ten įsteigtais juridiniais, Bendrovė privalo:

- gauti papildomą informaciją apie klientą ir naudos gavėją.
- gauti papildomą informaciją apie numatomą dalykinių santykių pobūdį.
- gauti informaciją apie kliento ir naudos gavėjo turto ir (ar) lėšų šaltinį.
- gauti informaciją apie numatomų ar įvykdytų sandorių priežastis.
- gauti vyresniojo vadovo patvirtinimą norint užmegzti ar tęsti dalykinius santykius su šiais klientais.
- vykdyti griežtesnę nuolatinę dalykinių santykių su šiais klientais stebėseną, padidinant taikytinų kontrolės priemonių skaičių ir laiką bei pasirenkant sandorių, kuriuos reikės toliau tirti, rūšis.
- užtikrinti, kad pirmas kliento mokėjimas būtų atliktas iš to kliento banko sąskaitos, mokėjimo ar elektroninių pinigų sąskaitos esančios Europos Sąjungoje arba trečiojoje valstybėje, kuriai taikomi lygiaverčiai kovos su PP reikalavimai ir priežiūra.

44. Kai sandoriai ar dalykiniai santykiai vykdomi su fiziniais ar juridiniais asmenimis iš valstybių, kurias FATF nurodė kaip turinčias didelę riziką, **ARBA** Bendrovė įvertina kliento riziką kaip didelę naudodama savo rizikos vertinimo formą, Bendrovė privalo:

- Gauti vyresniojo vadovo patvirtinimą norint užmegzti ar tęsti dalykinius santykius su šiais klientais.

- Nustatyti ir patvirtinti kliento turto šaltinį ir (arba) lėšas, susijusias su dalykiniais santykiais ar sandoriu.
- Vykdyti griežtesnę nuolatinę dalykinių santykių su šiais klientais stebėseną.
- Taikyti papildomas priemones Kovos su PP pareigūno nuožiūra:
  - ➢ gauti papildomą informaciją apie klientą ir naudos gavėją.
  - ➢ gauti papildomą informaciją apie numatomą dalykinių santykių pobūdį.
  - ➢ gauti informaciją apie numatomų ar įvykdytų sandorių priežastis.
  - ➢ užtikrinti, kad pirmas kliento mokėjimas būtų atliktas iš to kliento banko, mokėjimo ar elektroninių pinigų sąskaitos, esančios Europos Sąjungoje arba trečiojoje valstybėje, kuriai taikomi lygiaverčiai kovos su PP reikalavimai ir priežiūra.

XI. NUOLATINIS IŠSAMUS PATIKRINIMAS

45. Užmezgus dalykinius santykius su klientu, Bendrovė stebės dalykinius santykius siekiant užtikrinti, kad įvykdyti sandoriai atitinka Bendrovės turimą informaciją apie klientą, jo verslą, rizikos pobūdį ir lėšų šaltinį. Daugiau informacijos pateikiama Nuolatinio išsamaus patikrinimo (*angl. Ongoing Due Diligence*, toliau - NIP) procedūroje.

29. Bendrovė įvertina kiekvieno kliento rizikos balą ir priskiria rizikos koeficientą.

30. NIP reiškia, kad dokumentai, duomenys ar informacija, surinkti įvedimo proceso metu, yra atnaujinami ir susiejami peržiūrint esamus įrašus. Siekiant stebėti ir tikrinti santykius su klientais bei nustatyti neįprastą klientų veiklą, svarbu turėti atnaujintus PSK duomenis.

31. Kliento rizikos lygis lemia, kaip dažnai Bendrovė peržiūrės kiekvienus dalykinius santykius ir kaip dažnai bus atnaujinama ta informacija apie dalykinius santykius. Visiems santykiams su klientais reikalingas nuolatinis išsamus patikrinimas, tačiau didelės rizikos klientai bus stebimi dažniau.

32. Numatytas peržiūros dažnumas:

- didelės rizikos klientai bus peržiūrimi kas šešis mėnesius,
- vidutinės rizikos klientai bus peržiūrimi kasmet, ir
- mažos rizikos klientai bus peržiūrimi kas du metus.

50. Kiekvienų dalykinių santykių NIP yra skirtas:

- aptikti įtartiną veiklą, apie kurią reikia pranešti;
- nuolat atnaujinti klientų PSK informaciją, dalykinių santykių tikslą ir numatytą pobūdį bei informaciją apie naudos gavėjus;

- pakartotinai įvertinti rizikos, susijusios su kliento sandoriais ir veikla, lygį;
- nustatyti, ar sandoriai arba veikla atitinka anksčiau gautą informaciją apie klientą, įskaitant rizikos įvertinimą;
- laikui bėgant suprasti kliento veiklą tam, kad būtų galima išmatuoti bet kokius pokyčius siekiant nustatyti didelę riziką.

51. Šiems reikalavimams nereikia laikyti to paties laikotarpio, kol didelės rizikos klientai yra stebimi dažniau ir atidžiau nei mažos rizikos klientai. Didelės rizikos situacijų stebėjimas gali apimti tokias priemones kaip:

- sandorių peržiūra pagal patvirtintą tvarkaraštį, kuris apima vadovybės pasirašymą;
- ataskaitų rengimas arba dažnesnis ataskaitų, kuriose išvardinti didelės rizikos sandoriai, tikrinimas, veiklos ar veiklos pokyčių atsižvelgiant į lūkesčius žymėjimas, ir, jei reikia, abejonių kėlimas;
- verslo apribojimų ar parametrų, susijusių su sąskaitomis ar sandoriais, kurie sukeltų išankstinius įspėjimo signalus ir kuriuos privaloma peržiūrėti, nustatymas;
- dažnesnė sandorių pagal įtartinus su santykiais susijusius sandorių rodiklius peržiūra.

XII. SANKCIJŲ IRPOLITIŠKAI PAŽEIDŽIAMŲ (PAVEIKIAMŲ) ASMENŲ (PPA) PATIKRINIMAS

52. Lietuvos Respublika laikosi Europos Sąjungos, Jungtinių Tautų ir Jungtinių Valstijų nustatytų priemonių, kurių imamasi pagal Ekonominių ir kitų tarptautinių sankcijų įgyvendinimo įstatymą. Šios priemonės apima asmenų ir subjektų, kuriems taikomos sankcijos, sąrašą. Užsienio reikalų ministerija koordinuoja tarptautinių sankcijų įgyvendinimą Lietuvoje ir teikia informaciją apie tai.

33. Bendrovė turi patikrinti, ar klientai, klientų atstovai ar naudos gavėjai nėra įtraukti į asmenų, kuriems taikomos tarptautinės finansinės sankcijos, sąrašą.

34. Sankcijų sąrašai tikrinami tapatybės nustatymo etape Visi klientai dėl sankcijų yra nuolat tikrinami visu dalykinių santykių laikotarpiu ir sandorių metu.

35. Bendrovė laikysis Finansinių nusikaltimų tyrimo tarnybos prie Lietuvos Respublikos Vidaus reikalų ministerijos nurodymų dėl Tarptautinių finansinių sankcijų atitinkamo administravimo priežiūros reguliavimo srityje, patvirtintų FNTT direktoriaus 2016 m. spalio 20 d. sprendimu Nr. V-273 „Dėl tinkamo tarptautinių finansinių sankcijų įgyvendinimo finansinių nusikaltimų tyrimo tarnybos prie Lietuvos Respublikos Vidaus reikalų ministerijos reguliavimo srityje priežiūros nurodymų patvirtinimo“, todėl Bendrovė privalo:

- teikti informaciją apie finansinių sankcijų įgyvendinimą FNTT ir Lietuvos Respublikos Užsienio reikalų ministerijai;
- pateikti FNTT visus stebėsenai būtinus duomenis;
- paskirti darbuotoją (-us), kuris organizuotų finansinių sankcijų įgyvendinimą, būtų atsakingas už sąskaitų nutraukimą, reguliariai atnaujintų subjektų, kuriems

taikomos finansinės sankcijos, sąrašą, teiktų ataskaitas FNTT ir kitoms institucijoms, atsakingoms už tarptautinių sankcijų įgyvendinimo priežiūrą.

56. Bendrovė neužmegs dalykinių santykių su klientais, kuriems taikomos tarptautinės finansinės sankcijos. Išsamesnį procesą pateiktas Įvedimo procedūroje.

36. Bendrovė turi patikrinti, ar klientai, klientų atstovai ar naudos gavėjai nėra PPA.

37. PPA savanoriško deklaravimo forma yra įtraukta į kiekvieną PSK anketą ir siekiant patvirtinti iš kliento gautą informaciją, visų vardų bus ieškoma iš patikimų komerciškai ar viešai prieinamos informacijos šaltinių.

38. PPA statusas nėra įrodymas prieš asmenis ar subjektus. Tačiau tai priskiria klientą ar juridinį asmenį didelės rizikos kategorijai ir jam taikomas GIP.

39. Tokie klientai išlieka rizikingi mažiausiai vienerius metus po to, kai jie oficialiai nustojo būti PPA.

40. PPA patikra yra nuolatinis procesas visiems klientams, trunkantis visą dalykinių santykių laikotarpį.

XIII. ĮTARTINOS PINIGINĖS OPERACIJOS AR SANDORIAI

62. Įtartinos piniginės operacijos ar sandoriai nustatomi:

- pagal įtartinų piniginių operacijų ar sandorių nustatymo kriterijus, patvirtintus Finansinių nusikaltimų tyrimo tarnybos prie Lietuvos Respublikos Vidaus reikalų ministerijos direktoriaus 2014 m. gruodžio 5 d. sprendimu Nr. V-240 „Dėl galimo pinigų plovimo ir įtartinų piniginių operacijų ar sandorių atpažinimo kriterijų sąrašo patvirtinimo“.
- pastebint klientų veiklą, kuri dėl savo pobūdžio gali būti susijusi su pinigų plovimu ir (arba) teroristų finansavimu;
- nustatant kliento ir naudos gavėjo tapatybę;
- nuolat stebint kliento dalykinius santykius, įskaitant tų santykių metu įvykusių sandorių tyrimą.

63. Nustačius įtartiną piniginę operaciją ar sandorį, turi būti atliktas dokumentais pagrįstas tyrimas, ta operacija ar sandoris turi būti sustabdytas ir per tris darbo valandas nuo įtariamos veiklos nustatymo turi būti pateikta ataskaita FNTT. Tokiai ataskaitai nėra nustatytos minimalios ribos ar apribojimai. Kai FNTT pranešama apie įtartiną piniginę operaciją ar sandorį, jie privalo atsakyti per dešimt darbo dienų. Jei FNTT prašo papildomos informacijos, atsakymas į tą prašymą turi būti pateiktas nedelsiant.

41. Bendrovė praneša FNTT kliento tapatybės duomenis ir informaciją apie atliktus virtualiosios valiutos keitimo sandorius (virtualiosios valiutos pirkimas ar pardavimas nurodyta valiuta) arba sandorius virtualiąja valiuta (atsiskaitymai virtualiąja valiuta), piniginės operacijos ar sandorio vertė yra lygi arba didesnė nei 15 000 EUR arba ją atitinkanti

suma valiuta / virtualiąja valiuta, nepriklausomai nuo to, ar sandoris vykdomas atliekant vieną ar daugiau susijusių piniginių operacijų. Virtualiosios valiutos vertė nustatoma piniginės operacijos ar sandorio metu.

42. Tuo atveju, kai kliento piniginė operacija ar sandoris atitinka šios politikos 62 ir 64 punktų reikalavimus, Bendrovė pateikia FNTT pranešimą apie įtartiną piniginę operaciją ar sandorį ir pranešimą apie atliktą virtualiųjų valiutų keitimo operaciją arba sandorius virtualiąja valiuta, kai tokios piniginės operacijos ar sandorio suma yra lygi arba didesnė nei 15 000 EUR arba ją atitinkanti suma valiuta / virtualiąja valiuta, neatsižvelgiant į tai, ar sandoris įvykdytas vykdant vieną ar daugiau susijusių piniginių sandorių.

43. Pranešus paskirtam pareigūnui arba atitinkamai institucijai, bet koks veiksmas ar pasakymas, kuris gali „įspėti“ kitą asmenį, kad jis buvo atskleistas, arba pakenkti tyrimui, yra nusikalstama veika. Kai kliento paskyrai taikomas pranešimas apie įtartiną veiklą, bendraujant su klientu reikia imtis atsargių veiksmų ir papildomai pasikonsultuoti su Kovos su PP pareigūnu siekiant netyčia neatskleisti klientui tyrimo veiksmų.

44. Išsamus procesas aprašytas Sandorių stebėjimo procedūroje.

XIV. INFORMACIJOS IR DOKUMENTŲ SAUGOJIMAS

68. Tikslus įrašų saugojimas yra būtinas norint įrodyti visą su finansinių nusikaltimų rizikos valdymu susijusią veiklą ir sprendimus bei atitiktį PP prevencijai. Bendrovė privalo saugoti šiuos įrašus:

kliento tapatybės nustatymo įrašus;

- kliento tapatybės dokumentus ir naudos gavėjo duomenis;
- visus rizikos vertinimo įrašus ir kliento rizikos profilį;
- PSK anketą;
- visus įrašus, susijusius su NIP.

Sandorių įrašus:

- žurnalą, kuriame nurodyti sandorio duomenys dalykinių santykių metu;
- vidinius įtartinos veiklos tyrimus;
- pranešimų apie įtartiną veiklą teikimo žurnalą;
- virtualiosios valiutos keitimo sandorių arba sandorių virtualiąja valiuta, jei toks piniginis sandoris ar sandorio vertė yra lygi arba didesnė nei 15 000 EUR arba ją atitinkanti suma valiuta / virtualiąja valiuta, nepriklausomai nuo to, ar sandoris vykdomas per vieną ar daugiau susijusių piniginių sandorių, žurnalą;
- dalykinių santykių, nutrauktų dėl PP / TF priežasčių, žurnalą.

Kitus įrašus:

- įrodymus apie mokymo programas, susijusias su pinigų plovimu ir teroristų finansavimo prevencija, tiek vidaus, tiek išorės;
- kitus įrašus, jei to reikalauja Lietuvos pinigų plovimo prevencijos įstatymas ir kiti teisės aktai, susiję su pinigų plovimo / terorizmo finansavimo prevencija;

69. Duomenys registracijos žurnaluose turi būti įvesti chronologine tvarka, nedelsiant, bet ne vėliau kaip per 3 darbo dienas po piniginės operacijos ar sandorio įvykdymo.

3. Visi įrašai, susiję su pinigų plovimo ir teroristų finansavimo prevencija, turi būti saugomi elektroniniu būdu, lengvai prieinamu ir nuskaitomu formatu ir turi būti pateikiami nedelsiant, kai to paprašo kovos su PP pareigūnas arba atitinkamos išorės įstaigos, įskaitant kompetentingas institucijas. Bendrovė saugo su PP / TF prevencija susijusius įrašus elektroniniu būdu.

4. Įrašų saugojimo laikotarpis:

1.	Pateiktų pranešimų apie įtartiną veiklą žurnalas	Turi būti saugomas 8 metus po dalykinių santykių nutraukimo
2.	Virtualiosios valiutos keitimo operacijų arba sandorių, kurių suma yra lygi ar didesnė nei 15 000 EUR arba ją atitinkanti suma valiuta / virtualiąja valiuta, žurnalas	
3.	Visų kliento sandorių žurnalas	
4.	Dalykinių santykių, nutrauktų dėl PP / TF priežasčių, žurnalas	
5.	Tapatybės dokumentų kopijos, tapatybės nustatymo informacija ir PSK informacija	
6.	Skaitmeninės valiutos piniginės adresas kartu su savininko tapatybės informacija	
7.	Susirašinėjimas su klientu	Turi būti saugomas 5 metus po dalykinių santykių nutraukimo
8.	Patvirtinamieji iš kliento gauti dokumentai	Turi būti saugomi 8 metus po sandorio užbaigimo
9.	Vidaus tyrimo įrašai apie įtartinus sandorius	Turi būti saugomi 5 metus
10.	Mokymų žurnalas ir susiję dokumentai	Turi būti saugomi 5 metus nuo mokymų pabaigos

- Visos Kovos su PP pareigūno ataskaitos Generaliniam direktoriui ir Valdybai bus saugomos neribotą laiką.
- Bendrovė saugo visų darbuotojų gautų kovos su pinigų plovimu mokymų įrašus, jų pateikimo datą ir, jei taikoma, bet kokių bandymų rezultatus. Šie įrašai bus saugomi 10 (dešimt) metų nuo darbo Bendrovėje pabaigos.

- Visi pateikti pranešimai apie įtartiną veiklą, įskaitant susirašinėjimą su FNTT, Lietuvos banku (ar bet kuria kita vyriausybine institucija), bus saugomi neribotą laiką. Vidiniai pranešimai apie įtarimus bus saugomi 10 (dešimt) metų.

72. Įrašų saugojimo terminai gali būti papildomai pratęsti ne ilgiau kaip dviems metams pagrįstu kompetentingos institucijos nurodymu.

45. Registracijos žurnalai saugomi vadovaujantis Finansinių nusikaltimų tyrimo tarnybos prie Lietuvos Respublikos Vidaus reikalų ministerijos direktoriaus 2017 m. rugsėjo 4 d. sprendimu Nr. Dėl Kliento atliktų įtartinų ar neįprastų piniginių operacijų ir sandorių registracijos žurnalų tvarkymo taisyklių ir dideles nuolatines ir reguliarias pinigines operacijas apibūdinančių kriterijų nustatymo patvirtinimo“.

XV. ATITIKTIES MOKYMAI

74. Bendrovė turi kasmetinę mokymo programą visiems darbuotojams ir kitiems asmenims, kurie veikia Bendrovės vardu, siekiant užtikrinti kad tie, kurie bendrauja su klientais ir mato klientų sandorių veiklą, supranta ataskaitų teikimo, klientų tapatybės nustatymo ir įrašų tvarkymo reikalavimus.

46. Visi nauji Bendrovės darbuotojai privalo baigti kovos su pinigų plovimu ir teroristų finansavimu mokymus per įvadinio mokymo laikotarpį, kai jie prisijungia prie Bendrovės. Visi darbuotojai per pirmuosius šešis darbo mėnesius bus įtraukti ir išklausys visoje Bendrovėje vykdomus mokymus, susijusius su pinigų plovimo ir teroristų finansavimo prevencija, išskyrus darbuotojus, tiesiogiai susijusius su kovos su pinigų plovimu ir teroristų finansavimu priemonėmis. (pvz., Kovos su PP pareigūnas), kurie turi būti supažindinti su Bendrovės procedūromis prieš pradedant vykdyti funkcijas, susijusias su PP / TF prevencija.

47. Kovos su PP pareigūnas yra atsakingas už tai, kad visi būtų periodiškai informuojami apie kovos su PP / TF teisės aktų, politikos ir procedūrų pakeitimus ir esamą pinigų plovimo ar teroristų veiklos finansavimo schemų patobulėjimą, kurie yra ypač svarbūs jų darbui. Siekiant užtikrinti, kad darbuotojų mokymai būtų nuolat atnaujinami, visi esami darbuotojai reguliariai (bent per vienerius metus nuo paskutiniųjų mokymų) gaus tolesnius mokymus apie naujus ir esamus kovos su pinigų plovimu ir teroristų finansavimu bei reguliavimo reikalavimus.

48. Kovos su PP pareigūnas atnaujina darbuotojams paskirtų ir baigtų mokymų medžiagos žurnalą ir saugo jį penkerius metus (pvz., mokymų žurnalo ištrauką ar atsisiuntimą).

49. Atitinkami atitikties mokymai skirti visiems darbuotojams ir atitinkamiems užsakomųjų paslaugų teikėjams. Tai apima asmenis, dirbančius pardavimuose ir vyresniojoje vadovybėje, ir kitus asmenis, kuriems tenka atsakomybės pagal atitikties tvarką, pavyzdžiui, informacinių technologijų pareigūną ir kitus darbuotojus, atsakingus už elektroninių ar rankinių vidaus kontrolės priemonių kūrimą ir įgyvendinimą. Kovos su PP pareigūnas peržiūrės funkcijas ir suteiks tinkamus ir pritaikytus mokymus.

50. Bendrovės mokymai apims bent::

- Bendrą informaciją apie pinigų plovimo kontrolės priemones ir jų istoriją, įskaitant pinigų plovimo ir teroristų finansavimo apibrėžimus, kodėl nusikaltėliai tai daro ir kodėl svarbu juos sustabdyti.
- Teisinę informaciją apie tai, kokie su PP / TF prevencija susiję įstatymai yra taikomi institucijoms ir jų darbuotojams.
- Baudas už PP / TF prevencijos pažeidimus, įskaitant baudžiamąsias ir civilines nuobaudas, baudas, laisvės atėmimo bausmes, taip pat vidines sankcijas, pvz., drausmines nuobaudas iki darbo sutarties nutraukimo imtinai.
- Vidaus politikas, pvz., klientų tapatybės nustatymo ir patvirtinimo procedūras bei politikas, įskaitant klientų išsamų patikrinimą (KIP), griežtesnį išsamų patikrinimą (GIP) ir nuolatinį išsamų patikrinimą (NIP).
- Vidinio kovos su PP /TF ir sankcijų rizikos vertinimo peržiūrą.
- Teisinius įrašų tvarkymo reikalavimus.
- Įtartinų sandorių stebėjimo ir ataskaitų teikimo reikalavimus.
- Kaip reaguoti susidūrus su įtartinu klientu ar sandoriu.
- Kaip reaguoti į klientus, kurie nori apeiti ataskaitų teikimo reikalavimus.
- Darbuotojų pareigas ir atsakomybes.
- Konfidencialumo su PP / TF prevencija susijusiais klausimais išlaikymą.
- Kovos su PP / TF tendencijas ir kylančias problemas, susijusias su nusikalstama veikla, teroristų finansavimu ir reguliavimo reikalavimais.
- Pinigų plovimo schemas (pageidautina įmonėje ar panašiose institucijose įvykusius atvejus), įskaitant tai, kaip pirmą kartą buvo aptiktas veiklos modelis, jo poveikis įstaigai ir galutinis sprendimas.

80. Tam tikriems darbuotojams, pavyzdžiui, dirbantiems atitikties, klientų aptarnavimo ir operacijų srityse, reikalingi specialūs papildomi mokymai, kurie bus teikiami per išorines paslaugas arba viduje. Siekiant atitikti reikalavimus, mokymų programa bus peržiūrėta ir atnaujinta.