UAB "BALTIC CAPITAL PARTNERS"

POLICY ON THE PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

1. GENERAL PROVISIONS

1.1. The anti-money laundering and counter-terrorist financing policy (hereinafter – the Policy) of UAB "Baltic Capital Partners" (hereinafter – the Company) is designed to ensure that:

1.1.1. the identity of every client of the Company and their representative, where such identification is required, is established in accordance with the Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania and other applicable legal requirements;

1.1.2. potential money laundering and/or terrorist financing is prevented;

1.1.3. the transaction monitoring procedure is properly implemented;

1.1.4. The Company would cooperate only with reliable clients who do not pose reputational or financial risks;

1.1.5. the Company, in cooperation with the competent authorities, would comply with other requirements of legislation in force in the Republic of Lithuania.

1.2. The Policy has been drawn up in accordance with:

1.2.1. The Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania;

1.2.2. Order No. V-131 of 12 September 2017 of the Director of the Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania "on the approval of the Procedure for the Certification and Submission of Copies of Identity Documents";

1.2.3. 4 September 2017 Order No. V-129 of the Director of the Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania "on the approval of the Policy on the maintenance of cash transaction, transaction and customer registration logs" approved by Order No. V-129 of the Director of the Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania;

1.2.4. Order No. 1V-701 of the Minister of the Interior of the Republic of Lithuania of 16 October 2017 "on the procedure for suspending suspicious cash transactions or deals and submitting information on suspicious cash transactions or deals to the Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania, and on the submission of information on cash transactions and deals whose amount is equal to or exceeds 15,000 euros or the equivalent amount in foreign currency, to the Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania" "Procedures for the suspension of suspicious cash transactions or deals and the submission of information on suspicious cash transactions or deals to the Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania" and the "Procedures for the submission of information on cash transactions and deals amounting to or exceeding EUR 15,000 or the equivalent in foreign currency to the Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania";

1.2.5. Approved by Order No. V240 of the Director of the Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania dated 5 December 2014 "on the approval of the list of criteria for identifying possible money laundering and suspicious financial transactions or deals"

1.2.6. "List of criteria for identifying possible money laundering and suspicious financial transactions or deals".

1.2.7. Resolution No. 03-17 of the Bank of Lithuania of 12 February 2015 “On the Approval of Instructions for Financial Market Participants Aimed at Preventing Money Laundering and/or Terrorist Financing”.

2. TERMS

2.1. Close associate:

2.1.1. a natural person who is a participant in the same legal person or organisation without legal personality as a person holding or having held the positions referred to in point 2.14 of the Policy, or who maintains other business relations with such a person;

2.1.2. a natural person who is the sole beneficiary of a legal person or an organisation without legal personality established or operating de facto for the purpose of providing financial or other personal benefit to a person holding or having held the positions referred to in point 2.14 of the Policy.

2.2. Close family members – a spouse, a person with whom a registered partnership has been entered into (hereinafter – cohabiting partner), parents, brothers, sisters, children and their spouses, and the cohabiting partners of children.

2.3. Person – a natural or legal person of the Republic of Lithuania or a foreign state.

2.4. Responsible person – a person appointed by the Company’s director who is responsible for the implementation of the anti-money laundering and/or counter-terrorist financing measures set out in this Policy in the Company’s operations;

2.5. Company – UAB “Baltic Capital Partners”, company registration number 306386946, registered office at Konstitucijos pr. 7, Vilnius.

2.6. Business relationship – a commercial relationship between a client and the Company relating to their professional activities, which is intended to continue for a certain period of time.

2.7. Employee – any employee, service provider or partner of the Company who works directly with the Company’s clients.

2.8. FNTT – the Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania.

2.9. Suspicious financial transaction or deal – a financial transaction or deal involving assets which are suspected of having been obtained, directly or indirectly, from or through criminal activity and/or are suspected of being linked to terrorist financing.

2.10. Customer – a natural or legal person who uses the services provided by the Company.

2.11. Beneficial owner – a natural person who is the owner of, or exercises control over, a customer (a legal person or a foreign company), and/or a natural person on whose behalf a transaction or activity is carried out. The following are considered beneficial owners:

2.11.1. in the case of a legal person:

2.11.1.1. a natural person who owns the legal entity or who controls it directly or indirectly by holding a sufficient percentage of the shares or voting rights of that legal entity, including control through registered shares, except for public limited companies or collective investment undertakings ( ), whose securities are traded on regulated markets where requirements to disclose information about their activities in accordance with European Union legislation or equivalent international standards apply, or by controlling them in other ways. A natural person who holds 25 per cent plus one share or more than 25 per cent of a client’s ownership interest is considered a beneficial owner. The natural person(s) controlling a company or several companies which hold 25 per cent

plus one share or more than 25 per cent of the client's ownership interest shall be regarded as an indirect owner;

2.11.1.2. a natural person holding the position of senior manager, if the person referred to in subparagraph (a) of this paragraph has not been identified or if there is doubt as to whether the identified person is the beneficial owner;

2.12. A financial transaction – any payment, transfer or receipt of money.

2.13. Money laundering:

2.13.1. the alteration of the legal status of property or the transfer of property, knowing that such property is derived from or in connection with a criminal offence, with the aim of concealing or disguising the illicit origin of the property or of assisting any person involved in a criminal offence to evade the legal consequences of that offence;

2.13.2. concealing or disguising the true nature, source, location, disposition, movement, ownership or rights in respect of property, knowing that such property is derived from, or is related to, a criminal offence;

2.13.3. the acquisition, possession or use of property, knowing at the time of acquisition (or transfer) that such property was derived from or in connection with a criminal offence;

2.13.4. preparing, attempting or aiding and abetting any of the acts referred to in subparagraphs 1 to 3 of this paragraph.

2.14. Politically Exposed Persons (PEPs) – natural persons who hold (or have held within the last 12 months) important public functions, and their close family members or close associates.

2.15. AML/CFT Act – the Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania.

2.16. Significant public functions – functions in the Republic of Lithuania, the European Union, or in international or foreign institutions:

2.16.1. head of state, head of government, minister, deputy minister or assistant minister, state secretary, chancellor of parliament, government or a ministry;

2.16.2. Member of Parliament;

2.16.3. a member of a Supreme Court, Constitutional Court or other supreme judicial institution whose decisions are not subject to appeal;

2.16.4. the mayor of a municipality, the director of the municipal administration;

2.16.5. a member of the governing body of the supreme audit and control institution or the chairman, deputy chairman or a member of the board of the central bank;

2.16.6. an ambassador, a chargé d'affaires, the Commander of the Lithuanian Armed Forces, commanders of military forces and units, the Chief of the Defence Staff, or a high-ranking officer of the armed forces of a foreign state;

2.16.7. a member of the management or supervisory body of a state-owned enterprise, public limited company or private limited company in which the state holds, by right of ownership, shares or a portion of shares conferring more than half of all votes at the general meeting of shareholders of such companies;

2.16.8. municipal enterprises, public limited companies, private limited companies in which the municipality holds, by way of ownership, shares or a portion of shares conferring more than half of all votes at the general meeting of shareholders of such companies, and which are regarded as large enterprises under the Law on Financial Reporting of Enterprises of the Republic of Lithuania, a member of a management or supervisory body;

2.16.9. head of an international intergovernmental organisation, their deputy, or a member of the management or supervisory body;

2.16.10. the head of a political party, their deputy, or a member of the management body.

2.17. Terrorist financing – an act which constitutes a criminal offence under Article 2 of the International Convention for the Suppression of the Financing of Terrorism of 9 December 1999;

2.18. Third country – a financial institution supervised by competent authorities, another obliged entity, or a financial institution or other obliged entity registered in a Member State or a third country, meeting the following requirements:

2.18.1. they are subject to mandatory professional registration under the law;

2.18.2. they are registered in a Member State or a third country which applies requirements equivalent to those laid down by the European Union regarding the identification of customers and beneficial owners and the retention of information, and are supervised by competent authorities regarding compliance with these requirements.

2.19. A third country is a country that is not a Member State.

2.20. Member State – a country that is a member of the European Union or the European Economic Area;

2.21. Senior manager – an officer or employee holding a sufficiently senior position, possessing sufficient knowledge of the money laundering and/or terrorist financing risks faced by the institution or undertaking, and responsible for taking decisions that may affect those risks.

2.22. Other terms not defined in this section of the Policy shall be understood as defined in the PPTFPĮ.

3. IDENTIFICATION OF THE CUSTOMER AND BENEFICIAL OWNER

3.1. The Company must take measures to identify the customer and the beneficial owner in the following cases:

3.1.1. before entering into a business relationship relating to an activity subject to the requirements set out in this Policy;

3.1.2. where there are doubts as to the accuracy or authenticity of previously obtained customer and beneficial owner identification data;

3.1.3. in any other case where there are suspicions that money laundering and/or terrorist financing activities are being, have been, or will be carried out.

3.2. A company employee must provide the customer – or, if the customer is a legal entity, the customer's director or authorised representative – with a customer questionnaire to complete, which requests the information necessary to establish the identity of the customer and the beneficial owner. Once the client or their representative has completed the questionnaire, the employee checks that all fields have been filled in. If any fields are left blank or the answers in certain fields are unclear or vague, the employee must ask for the information to be provided or clarified. The questionnaire completed by the customer is used in the process of identifying the customer and the beneficial owner and assessing the risks posed by the customer and the beneficial owner. The purpose of providing the questionnaire to the customer for completion is to gather as much information as possible about the customer, their business partners, the origin of their assets and funds, the business relationships they are developing, and the scope of these relationships.

3.3. In all cases where the Company suspects that a client is not acting on their own behalf, the Employee must take all appropriate, targeted and proportionate measures to determine whether the customer is acting on their own behalf or is being controlled, and to identify the beneficial owner, as well as, if the customer is acting through a representative, the identity of the customer's representative. To this end, the Employee must ask questions not only directly about beneficial owners and shareholders, but also about the business model, its operation, future plans and planned investments. If an Employee notices that the person with whom they are communicating does not know the answers to some of the questions relating to the conclusion of the contract, the information required for its

conclusion, or lacks sufficient knowledge to substantiate the answers provided, must inform the Company's director of this and take action agreed with the director to further verify the beneficiary's identity.

3.4. When verifying the identity of the client and the beneficial owner, the employee must request from them documents and other data on the basis of which the Company can understand the management structure and nature of the business of the client, which is a legal entity, as well as obtain information regarding the purpose and intended nature of the client's business relationship, and verify the identity of the client and the beneficial owner.

3.5. In all cases where the identity of the customer and the beneficial owner is established, a Company employee must verify them on the basis of documents, data or information obtained from reliable sources and monitor the business relationship. To ensure that the documents, data or information provided at the time of establishing the identity of the customer and the beneficial owner are appropriate and up to date, they must be reviewed and updated on a regular basis.

3.6. Employees are prohibited from entering into business relationships where they are unable to meet the requirements set out in this paragraph:

3.6.1. if the customer fails to provide data confirming their identity, if they provide incomplete data or if the data is incorrect, if the customer or their representative refuses to provide the information necessary to establish their identity, conceals the identity of the beneficial owner or refuses to provide the information necessary to establish the identity of the beneficial owner, or if the information provided is insufficient;

3.6.2. if the Company is unable to ensure proper compliance with the requirements set out in clauses 3.3 to 3.5 of the Policy. In such cases, having assessed the risk of money laundering and terrorist financing, the Employee must immediately notify the Company's director, and the director, where there are grounds to do so, must also notify the FNTT;

3.6.3. It is also prohibited to enter into business relations if, following a customer check, it is established that the customer is associated with persons, groups of persons, companies and/or institutions subject to sanctions imposed by the United Nations, the European Union and other international organisations. Checks can be carried out on the website of the Ministry of Foreign Affairs of the Republic of Lithuania (https://www.urm.lt/sankcijos).

3.7. If a customer evades or refuses to provide the Employee, at the Employee's request and within the specified time limits, with information regarding the origin of funds or assets, or other additional data, an Employee of the Company may initiate the suspension of business relations with the client until the requested information is provided, or the termination of business relations with the client, by informing the Director of these circumstances. The decision to suspend or terminate business relations with the client is taken by the Director. Where a customer maliciously fails to provide the requested information, evades providing information on the origin of funds and assets, or provides false information, the director shall decide to terminate the business relationship with the customer.

3.8. An employee must immediately re-verify the customer's identity by applying enhanced customer due diligence in the following cases:

3.8.1. where the customer provides information for the purpose of identification, knowing that it is incorrect;

3.8.2. where the customer conceals information;

3.8.3. where circumstances arise requiring enhanced customer identification in the cases set out in clause 7.2 of the Policy.

3.9. If it transpires that a customer has provided information to establish their own identity or that of a beneficiary whilst knowing it to be incorrect, or if a customer conceals information, the Employee must ascertain the reasons why the incorrect information was provided and immediately inform the Company's director of these circumstances. The Company Director must analyse the information provided within 2 (two) working days and, having established that the client's actions may have

involved attempts to conceal certain information with a view to carrying out unlawful activities, report this client and their actions to the FNTT.

3.10. Information regarding clients whose identity is established in accordance with the provisions of Chapter 6 of the Policy, and the beneficial owners of such clients, must be updated at least every 2 (two) years.

3.11. If it is established that the beneficial owner is a natural person other than that specified in clause 3.10 of the Policy, the Employee must inform the Director thereof. Business relations with such clients shall only be commenced upon receipt of the Director's approval.

3.12. The Company shall not be liable to the client for failure to fulfil contractual obligations or for any loss or damage arising from the non-execution of the client's financial transactions or deals, if the Company failed to execute the client's financial transactions or deals for the reasons specified in this Policy.

4. IDENTIFICATION OF THE CLIENT IN THE PRESENCE OF THE CLIENT

4.1. When verifying a customer's identity in person, staff shall require the customer – a natural person – to present an identity document issued by the Republic of Lithuania or a foreign state, or a residence permit for the Republic of Lithuania, or the Directive of the European Parliament and of the Council of 20 December 2006 Directive 2006/126/EC of the European Parliament and of the Council on driving licences (recast), issued in a European Economic Area country and containing the following data confirming his identity (hereinafter referred to as an identity document): first name(s), surname(s), personal identification number (for a foreign national – date of birth (if available – personal identification number or other unique sequence of characters assigned to that person for identification purposes), the number and period of validity of the residence permit in the Republic of Lithuania, the place and date of issue (applicable to foreign nationals), a photograph, a signature (except where this is not required in the identity document), nationality (except where this is not required in the identity document); if the person is stateless, the country that issued the identity document. Where the identity document does not specify the customer's nationality, a Company employee, when verifying the identity of a customer who is a natural person in their physical presence, must request details of the customer's nationality.

4.2. Where the customer is a legal entity represented by a natural person, or where a natural person is represented by another natural person, the identity of these representatives shall be verified in the same way as that of a natural person acting as a customer. The customer must also provide information about the head of the legal entity: the head's first name, surname, personal identification number (for a foreign national – date of birth (if available, the personal identification number or other unique sequence of characters assigned to that person for identification purposes), nationality (if the person is stateless, the country that issued the identity document).

4.3. Staff shall require the client – a legal person – to provide identity documents containing the following details: name, legal form, registered office, address of actual business operations, code (if assigned), registration extract and its date of issue, details of representatives acting on behalf of the legal entity under a power of attorney, as specified in clause 4.2 of the Policy, the legal entity's types of activity, the purposes and subject matter of the business relationship, and the nature of its economic and commercial activities.

4.4. The Company is entitled to obtain the documents, data or information necessary to verify the identity of the customer and the beneficiary, as specified in clauses 4.1 to 4.3 of the Policy, directly from government information systems or registers, and not to require the customer to submit these documents, data or information, provided that the customer confirms the Company's documents, data or information obtained directly from state information systems or registers with a signature (including a qualified electronic signature). A Company employee may not require the customer to sign documents, data or information received by the Company directly from state information systems or registers with a signature if such documents, data or information do not differ from documents, data

or information previously confirmed by the client's signature, if the documents, data or information obtained from state information systems or registers concern the head of a legal person, and also if such documents, data or information are obtained from the Population Register of the Republic of Lithuania, and where such data are certified by the signature of a state institution.

4.5. When commencing the customer identification process, where the customer is a natural person or a representative of a legal person and is physically present during the identification process, the Employee must:

4.5.1. assess whether the customer (or the customer's representative) – a natural person commencing cooperation with the Company – presents valid identity documents; determine whether the document presented contains a photograph of that specific customer. Upon receiving an identity document issued in the Republic of Lithuania, the Employee shall check it against the database of invalid identity documents (https://www.ird.lt/lt/paslaugos/informacijos-rinkmenos/paieska-negaliojanciu-asmens-dokumentu-duomenu-bazeje). If the Employee determines that the identity document is invalid, they must request a valid identity document;

4.5.2. assess the condition of the document presented (paying particular attention to whether the photograph, pages or entries have been altered, corrected, or similar);

4.5.3. ascertain whether the client – a natural or legal person – will use the Company's services themselves or whether they will represent the interests of another person;

4.5.4. verify whether a natural or legal person has the necessary authorisation to act on behalf of the customer;

4.5.5. make a copy or scan the pages of the identity document presented by the natural person which contain the photograph of that natural person and other data necessary to establish their identity;

4.5.6. where it is necessary to verify the identity of a foreign client, make a copy of the identity document and the page of the corresponding residence permit in the Republic of Lithuania containing a photograph, or scan the document;

4.5.7. in accordance with the procedure set out in the Policy, take steps to justify the need to apply enhanced identity verification.

4.6. If the client is a legal entity represented by a natural person, or if a natural person is represented by another natural person, the employee must request a power of attorney from them and verify its validity (i.e. the right of the person issuing it to issue such a power of attorney), the duration of the power of attorney, and the actions specified in the power of attorney (the power of attorney must comply with the requirements of the Civil Code of the Republic of Lithuania; it must specify the date of issue and be certified by the legal entity's seal, if the legal entity is required to have a seal; a power of attorney issued abroad must be legalised or certified by an apostille).

4.7. To establish identity, the originals of the documents or copies of these documents certified by notaries, consular officials of the Republic of Lithuania or other state institutions must be submitted.

4.8. If a client who is a legal entity is represented by another legal or natural person and the grounds for such representation are set out in the client's founding documents, the Company's employees must verify the document appointing the person to the relevant governing body of the client and review the relevant section of the client's founding documents (articles of association, etc.) confirming such facts, or review an extract from the register confirming that the person is authorised to act on behalf of the client.

4.9. Whenever a business relationship with a client is established, the Company's employees are required to inform the client of their obligation to notify the Company immediately in writing of any revocation, expiry or change in the scope of their representative's authority. Until such information is provided to the Company, the representative's powers of attorney shall be deemed not to have expired, unless the Company knew or ought to have known of the revocation, expiry or change in the scope of the client's representative's powers of attorney.

5. REMOTE CUSTOMER IDENTIFICATION

5.1. The Company may verify the identity of the client and the beneficial owner where the identity of the client and the beneficial owner is verified without their physical presence and using electronic means that allow for live video transmission in one of the following ways:

5.1.1. using third-party information about the customer or beneficial owner;

5.1.2. using electronic identification means issued in the European Union that operate in accordance with electronic identification schemes of a high or sufficient security assurance level, as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;

5.1.3. where information regarding a person's identity is authenticated by a qualified electronic signature using a qualified certificate for electronic signatures that complies with the requirements of Regulation (EU) No 910/2014. Qualified electronic signatures from third countries, created using a qualified electronic signature certificate, shall be recognised in accordance with Article 14 of Regulation (EU) No 910/2014.

5.1.4. using electronic means that allow for live video transmission in one of the following ways:

5.1.4.1. during the live video transmission, the original of the Customer's identity document is captured and the Customer's identity is verified using an advanced electronic signature that meets the requirements set out in Article 26 of Regulation (EU) No 910/2014;

5.1.4.2. during a live video call, an image of the Customer's face is captured and the original identity document presented by the Customer is verified.

5.2. When verifying the identity of the customer and the beneficiary in the cases specified in clauses 5.1.1. to 5.1.3. of this Policy, the Company must comply with the following conditions:

5.2.1. prior to verifying the identity of the customer and the beneficial owner in the cases specified in clauses 5.1.1. – 5.1.2. of this Policy, the customer's identity was established by a Third Party in their physical presence or using electronic means allowing for live video transmission in one of the ways specified in clause 5.1.4. of this Policy, as well as where the customer's identity was established through their physical presence when issuing an electronic identification means operating under an electronic identification scheme with a high or sufficient level of security;

5.2.2. 5.2.1. prior to verifying the identity of the customer and the beneficiary in the cases specified in clauses 5.1.1–5.1.3 of this Policy, the identity of the customer and the beneficiary – a natural person and a representative of a legal person – was verified using the documents specified in Chapter 4 of this Policy.

5.3. When verifying the identity of the customer and the beneficial owner in accordance with Section 5 of the Policy, Employees must take the measures set out in Section 4 and establish and verify the identity of both the customer and the beneficial owner, use additional data, documents or information to establish the identity of the customer and the beneficial owner, which would allow them to verify the authenticity of the customer's identity and check whether there are circumstances requiring enhanced customer identification.

5.4. The Company may engage third parties and utilise the technological solutions they offer to verify the customer's identity without the customer being physically present. In such cases, the Company ensures that all information collected during the verification of the customer's and beneficiary's identity is transferred to the Company and stored in the customer's file.

5.5. When verifying the customer's identity, the Company may also use the services of third parties and the information they provide. Before verifying the identity of the customer and the beneficial owner based on information from third parties, the Company must ensure that:

5.5.1. the client's identity has been verified by the third party in one of the following ways:

5.5.1.1. in their physical presence, using an identity document, or an extract from the register of legal entities, or the legal entity's incorporation documents;

5.5.1.2. using electronic means that allow for live video transmission;

5.5.1.3. by making a payment to the Third Party's payment account from an account held in the Customer's name at a credit institution registered in a Member State or in a Third Country that has established requirements equivalent to those of the Law, and which is supervised by the competent authorities regarding compliance with these requirements, and by submitting a paper copy of an identity document certified in accordance with the procedure laid down in the laws of the Republic of Lithuania;

5.5.2. The Third Party shall, upon the Company's request, immediately provide all requested information and data required to comply with the requirements for identifying the Customer or Beneficiary set out in the PPTFPĮ and the Policy;

5.5.3. The Third Party, upon request by the Company, shall immediately provide copies of documents relating to the identification of the customer or beneficiary, and other documents relating to the customer or beneficiary, which are required to be held in accordance with the requirements for identifying the customer or beneficiary set out in the PPTFPĮ and the Policy.

5.6. When selecting a third country whose information will be relied upon to identify the customer and the beneficial owner, the Company takes into account the fact that the responsibility for complying with the requirements of the PPTFPĮ and the Policy regarding the identification of the customer or beneficial owner lies with the Company.

6. IDENTIFICATION OF THE BENEFICIAL OWNER

6.1. When verifying the identity of a customer, the beneficial owner must be identified in all cases. Identifying the beneficial owner in all cases means identifying a natural person or a group of natural persons.

6.2. When verifying the identity of the beneficial owner, where the identity of both the customer and the beneficial owner is verified in the customer's physical presence, employees must request the following identity details from the customer and the beneficial owner: first name(s), surname(s), personal identification number (for a foreign national – date of birth (if available – personal identification number or other unique sequence of characters assigned to that person for identification purposes, number and expiry date of the residence permit in the Republic of Lithuania, place and date of issue), nationality (if the person is stateless – the country that issued the identity document).

6.3. Employees verify the documents and information provided by the client regarding the beneficiary, based on documents, data or information obtained from a reliable and independent source. Such actions by the Employee also include requesting the customer to specify public sources where information about the beneficiary could be verified.

6.4. The client confirms the accuracy of the data provided by their signature and/or seal (if they are required to have a seal under the legislation governing their activities).

6.5. If the customer's identity is established without the customer being physically present, the customer (if a natural person) or the representative of the customer (if a legal person) must provide the information about the beneficial owner specified in clause 6.2 of the Policy.

6.6. The company is required to collect and, upon request by the FNTT, provide the following information about the beneficiary:

6.6.1. the beneficiary's identity details;

6.6.2. evidence of the verification of the information provided by the customer;

6.6.3. information on the ownership and control structure of the customer (legal person).

6.7. The identity of the beneficial owner must be established before the completion of the customer identification procedure.

6.8. When establishing the identity of the beneficial owner, additional information must be obtained from the Information System on Participants in Legal Entities (JADIS), from which data on that client's beneficial owners must be retrieved. The company also has the right to access other state information systems and registers in which data on participants in legal entities is stored. If a discrepancy is identified between the information on the beneficial owners of a client – a legal person – provided in the Information System on Participants in Legal Entities (JADIS) and the information held by the company regarding the beneficial owners of the same client, the employee must notify the client of this and suggest that they provide accurate information about their beneficial owners to the administrator of the Information System on Participants in Legal Entities (JADIS). Until the information provided by the client matches the information published in the Information System of Participants in Legal Entities (JADIS), or if the Information System of Participants in Legal Entities (JADIS) contains no data on the client's beneficial owners, business relations with the client shall not be initiated.

7. ENHANCED CUSTOMER IDENTIFICATION

7.1. Prior to the customer identification procedure, the Employee checks whether there are circumstances requiring enhanced customer identification.

7.2. Enhanced customer identification is carried out:

7.2.1. when transactions or business relationships are conducted with politically exposed persons;

7.2.2. if, upon assessing the factors set out in clause 7.8 of the Policy, a higher risk of money laundering and/or terrorist financing is identified. If a customer meets at least one of the factors specified in clause 7.8 of the Policy, they are considered to pose a higher risk of money laundering and/or terrorist financing;

7.2.3. where transactions or business relationships are conducted with natural persons residing in high-risk third countries identified by the European Commission or with legal entities established there;

7.2.4. where transactions or business relationships are conducted with natural persons residing in high-risk third countries identified by the Financial Action Task Force on Money Laundering and Terrorist Financing as having serious deficiencies in the prevention of money laundering and (or) the prevention of terrorist financing and the prevention of these offences.

7.3. When carrying out enhanced customer due diligence in business relationships with politically exposed persons, the Employee must:

7.3.1. verify whether this person, their representative, beneficial owner or their close family members and close associates are politically exposed persons or have been so in the last 12 months;

7.3.2. verify the information specified in sub-clause 7.3.1 of the Policy regarding the client and their representative, beneficiary or their close family members and close associates using reliable public search sources;

7.3.3. verify the answers provided by the client in the questionnaire regarding politically exposed persons;

7.3.4. take appropriate measures to determine the source of assets and funds related to the business relationship or transaction – ask the client to explain the origin of these funds and to provide documents supporting the client's statements, where the Employee deems this necessary;

7.3.5. obtain the approval of the Company's director to establish or continue business relationships with such clients when they become politically exposed persons;

7.3.6. carry out enhanced ongoing monitoring of business relationships with politically exposed persons.

7.4. When a politically exposed person ceases to hold a prominent public position, the Company must continue to take into account the risk posed by that person for a period of not less than 12 months and apply appropriate measures tailored to the level of risk until it is established that the person no longer poses the risk characteristic of politically exposed persons.

7.5. A company implementing the requirements set out in this chapter shall be entitled to receive from the Chief Official Ethics Commission the available data on politically exposed persons (influenced) who have been entrusted with important public duties in the Republic of Lithuania, who are required by law to declare their public and private interests, and whose declaration data is public. You can carry out a check by clicking on this link https://pinreg.vtek.lt/app/.

7.6. When applying enhanced customer due diligence in transactions or business relationships with natural persons residing in high-risk third countries as defined by the European Commission, or with legal entities (or their beneficial owners) established there, the Employee must:

7.6.1. obtain additional information about the customer and the beneficial owner;

7.6.2. obtain additional information regarding the nature of the proposed business relationship;

7.6.3. to obtain information on the source of the client's and the beneficiary's funds and assets;

7.6.4. obtain information regarding the reasons for proposed or completed transactions;

7.6.5. obtain the director's approval to establish business relationships with these clients or approval to continue business relationships with these clients;

7.6.6. carry out enhanced ongoing monitoring of business relationships with these customers, by increasing the number and frequency of control measures applied and by identifying the types of transactions that will require further investigation;

7.6.7. ensure that the customer's first payment is made from an account held by that customer with a credit, payment or electronic money institution, where the credit, payment or electronic money institution is registered in a Member State of the European Union or in a third country that has established requirements equivalent to those of the AML/CFT Directive, and the competent authorities supervise its compliance with those requirements.

7.7. When applying enhanced customer due diligence in cases where transactions or business relationships are conducted with natural persons residing in high-risk third countries identified in the lists published by the Financial Action Task Force on Money Laundering and Terrorist Financing of countries with serious deficiencies regarding the prevention of money laundering and/or the prevention of terrorist financing and the prevention of these offences, as well as in cases where the Company's risk assessment and management procedures identify a higher risk of money laundering and/or terrorist financing, The employee shall take one or more additional measures to verify the identity of the customer and the beneficial owner in order to mitigate the emerging risk and must:

7.7.1. obtain the director's approval to establish business relations with these customers or approval to continue business relations with these customers;

7.7.2. request detailed explanations regarding the beneficial owner and their activities outside the Republic of Lithuania, as well as assets or funds related to the business relationship;

7.7.3. The Company is entitled to enter into business relationships only with persons carrying out activities in the Republic of Lithuania;

7.7.4. to carry out enhanced ongoing monitoring of business relationships with these customers.

7.8. When determining whether there is an increased risk of money laundering and/or terrorist financing, the Company's employees must assess at least the following factors:

7.8.1. customer characteristics:

7.8.1.1. the customer's business relationship is conducted under unusual circumstances without any apparent economic or legitimate purpose;

7.8.1.2. other persons are paying on behalf of the customer and there is no logical explanation for this;

7.8.2. characteristics of the product, service, transaction or service delivery channel:

7.8.2.1. a transaction is entered into where the assets of a third party, unrelated to the customer or the beneficiary, are pledged to secure its performance, and the customer fails to provide a rational explanation as to why such a transaction is being entered into;

7.8.3. territorial characteristics:

7.8.3.1. based on data from reports or similar documents of the Financial Action Task Force on Money Laundering and Terrorist Financing or a regional organisation of a similar nature, significant non-compliance of the state's anti-money laundering and counter-terrorist financing system with international requirements has been identified;

7.8.3.2. based on data from governmental and widely recognised non-governmental organisations that monitor and assess levels of corruption, a high level of corruption or other criminal activity has been identified in the country;

7.8.3.3. the country is subject to sanctions, embargoes or similar measures imposed, for example, by the European Union or the United Nations;

7.8.3.4. the state finances or supports terrorist activities, or terrorist organisations included on lists drawn up by international organisations are operating within the territory of the state.

8. SIMPLIFIED CUSTOMER IDENTIFICATION

8.1. Simplified customer identification is carried out in the cases provided for in Article 15 of the PPTFPĮ.

8.2. When applying simplified customer identification, the Company:

8.2.1. collects the following data:

8.2.1.1. from the customer – a natural person: first name(s), surname(s), personal identification number (for a foreign national – date of birth (if available – personal identification number or other unique sequence of characters assigned to that person for identification purposes), residence permit number in the Republic of Lithuania and its validity period, place and date of issue (applicable to foreign nationals);

8.2.1.2. for a client that is a legal person: name, legal form, registered office, address of actual business operations, code (if assigned).

8.2.2. ensures that the client's first payment is made from an account held with a credit, payment or electronic money institution, where the credit, payment or electronic money institution is registered in a Member State of the European Union or in a third country that has established requirements equivalent to those of the AML/CFT legislation, and the competent authorities supervise its compliance with these requirements.

8.3. The Company shall not apply simplified customer due diligence where the circumstances set out in Section 7 of this Policy apply, in which case enhanced customer due diligence must be carried out.

8.4. If, in the course of ongoing monitoring of a customer's business relationship, it is determined that the risk of money laundering and/or terrorist financing is no longer low, the Company must take the measures set out in this Policy and establish and verify the identity of both the customer and the beneficial owner.

9. MONITORING OF BUSINESS RELATIONSHIPS AND IMPLEMENTATION OF INTERNATIONAL FINANCIAL SANCTIONS AND RESTRICTIVE MEASURES

9.1. Upon establishing business relationships with customers falling within the scope of the PPTFPĮ Act, the Company carries out routine or enhanced ongoing monitoring of transactions and the business relationships of such customers:

9.1.1. Standard monitoring of transactions and business relationships is carried out for customers whose identity has been established using the standard customer identification procedures set out in this Policy. In this case, ongoing monitoring of client transactions is carried out and, provided no suspicions arise, the data provided by clients and the data from independent sources used to verify it are reviewed and updated periodically, but at least once a year;

9.1.2. enhanced monitoring of transactions and business relationships is carried out for customers whose identity has been established using the enhanced customer identification procedures set out in this Policy. In this case, ongoing monitoring of customer transactions is carried out and, provided no suspicions arise, the data provided by customers and the data from independent sources used to verify it are reviewed and updated periodically, but at least twice a year.

9.2. In carrying out ongoing monitoring of transactions and customer business relationships (both standard and enhanced), the Company shall in all cases:

9.2.1. carries out identity checks on customers, their representatives and beneficiaries;

9.2.2. carries out checks on transactions entered into during the course of business relations to ensure that the transactions carried out are consistent with the Company's knowledge of the customer, their business, the nature of the risk and the source of funds;

9.2.3. immediately takes measures to prevent money laundering and/or terrorist financing.

9.3. Where the Company's employees determine that a client or beneficial owner is included in the lists referred to in during the course of the business relationship, the Company's employees shall:

9.3.1. shall immediately cease the performance or execution of obligations arising prior to the determination that the customer or beneficial owner is included in the lists referred to in clause 3.6.3 of this Policy, or suspend their performance;

9.3.2. shall immediately unilaterally terminate transactions entered into prior to the determination that the customer or beneficial owner is included in the lists referred to in clause 3.6.3 of this Policy, or suspend their execution;

9.3.3. notify the FNTT thereof within 3 hours;

9.3.4. provide the FNTT with all data necessary for the performance of its supervisory duties.

10. REPORTING OF SUSPICIOUS FINANCIAL TRANSACTIONS OR TRANSACTIONS

10.1. An FNTT employee shall submit a report containing information on suspicious financial transactions or deals by email. The employee must provide the FNTT with:

10.1.1. data confirming the identity of the customer or their representative (if the financial transaction is carried out through a representative) (for a natural person – first name, surname, personal identification number (for a foreign national – date of birth, and, if available, personal identification number or other unique sequence of characters assigned to that person for identification purposes); for a legal person – name, legal form, registered office address, and registration number, if such a number has been assigned);

10.1.2. which FNTT-approved criterion, set out in the legal act referred to in sub-paragraph 1.2.5 of the Policy, the transaction meets;

10.1.3. the method of carrying out the suspicious financial transaction, if a suspicious financial transaction is being reported;

10.1.4. the date and value of the suspicious financial transaction or transaction;

10.1.5. the contact details of the customer and their representative (if the financial transaction is carried out through a representative) (telephone numbers, email addresses, contact persons, their telephone numbers and email addresses);

10.1.6. . the entity in whose favour the suspicious financial transaction or transaction is carried out (for a natural person – first name, surname, personal identification number (for a foreign national – date of birth, and, if available, personal identification number or other unique sequence of characters assigned to that person for identification purposes); for a legal person – name, legal form, registered office address, registration number);

10.1.7. the date and time when the suspicious financial transaction was suspended;

10.1.8. if the suspicious financial transaction was not suspended, the reasons why it was not suspended;

10.1.9. any other information deemed important by the Employee.

10.2. Employees must, without delay and no later than within 1 working day of such knowledge or suspicions arising, notify the director and the FNTT if they know or suspect that any amount of funds has been obtained directly or indirectly from a criminal offence or through participation in such an offence, as well as if they know or suspect that the funds are intended to support one or more terrorists or a terrorist organisation.

10.3. Company employees who determine that a customer is carrying out a suspicious financial transaction, regardless of the amount of the transaction, must suspend that transaction and, no later than within 3 working hours of the suspension of the transaction, report the transaction to the director, who shall then inform the FNTT.

10.4. Employees who receive information that a customer intends to or is attempting to carry out a suspicious financial transaction must immediately inform the director, and the director must inform the FNTT.

10.5. Upon receiving a written instruction from the FNTT to suspend suspicious financial transactions or deals carried out by a customer, the company must suspend such transactions or deals for up to 10 working days from the time specified therein or from the moment specific circumstances arise.

10.6. If, within 10 working days of the submission of the notification or receipt of the instruction, the Company is not required to comply with the temporary restriction of ownership rights in accordance with the procedure laid down in the Code of Criminal Procedure of the Republic of Lithuania (hereinafter referred to as the Code of Criminal Procedure), the financial transaction or deal must be resumed. Prior to the expiry of this period, financial transactions may only be resumed upon written instruction from the FNTT.

10.7. Upon receipt of a notification from the FNTT that a suspicious financial transaction carried out by a customer must be completed, the Employee shall immediately take steps to lift the suspension of the suspicious financial transaction.

10.8. The Company must provide the information requested by the FNTT within 1 working day of receiving the request.

11. CLASSIFICATION OF CUSTOMERS INTO RISK GROUPS

11.1. The Company classifies Customers into the following groups:

11.1.1. those posing a low risk of money laundering and/or terrorist financing;

11.1.2. those posing a medium risk of money laundering and/or terrorist financing; and

11.1.3. posing a high risk of money laundering and/or terrorist financing.

11.2. The Company's customers are classified as posing a medium risk of money laundering and/or terrorist financing, except in cases where:

11.2.1. there are grounds for classifying them as posing a low risk of money laundering and/or terrorist financing; or

11.2.2. there are grounds for classifying them as a customer group posing a high risk of money laundering and/or terrorist financing.

11.3. A customer is assigned to a risk group following an assessment based on the criteria set out below:

No.	CRITERION	VALUE	SCORE
1.	Legal status	Natural person	0
		Legal entity	1
2.	Resident status	The client's country of residence / the principal's country / the shareholder's country / the beneficial owner's country is Lithuania	0
		The client's country of residence / the principal's country / the shareholder's country / the beneficial owner's country is not Lithuania	1
3.	PEP status	The customer is not a PEP	0
		The customer is a PEP	2
4.	New legal entity	The customer is a legal entity established more than 365 days ago	0
		The client is a legal entity established less than 365 days ago	1
5.	Compliance with the criteria set out in clause 7.8 of the Policy	The customer does not meet any of the criteria set out in clause 7.8 of the Policy	0
		The customer meets at least one of the criteria set out in clause 7.8 of the Policy	2

11.4. Based on the number of points scored, the customer is assigned to this risk group:

11.4.1. posing a low risk of money laundering and/or terrorist financing, if they have scored no more than 1 point;

11.4.2. posing a medium risk of money laundering and/or terrorist financing, if they have scored between 2 and 3 points;

11.4.3. posing a high risk of money laundering and/or terrorist financing, if they have scored 4 points or more.

11.5. Criteria according to which (if at least one criterion is met) a Customer is considered to pose a high risk of money laundering and/or terrorist financing:

11.5.1. at the time of identification, the customer refuses to take the steps necessary to establish their identity and provide information about themselves and their business;

11.5.2. the customer fails to provide documents confirming their financial activities at the Company's request;

11.5.3. the data used to verify the identity of the customer or the customer's representative (if the financial transaction is carried out through a representative) corresponds to the data on persons associated with money laundering and/or terrorist activities, as set out in the lists drawn up by the Republic of Lithuania and international organisations (FATF, the United Nations, the European Union) relating to persons involved in money laundering and/or terrorist activities, or that financial sanctions apply to them under the Law on the Implementation of Economic and Other International Sanctions of the Republic of Lithuania;

11.5.4. The Company determines that there are signs not typical of the customer's usual activities (financial transactions involving large sums of money, the customer frequently enters into new loan agreements and repays them after a short period of time, etc.);

12. STORAGE AND PROTECTION OF INFORMATION

12.1. The Company must maintain a register of suspicious financial transactions or deals and the dispatch of reports thereon to the FNTT (Appendix No. 1). Data shall be entered into the register in chronological order, based on documents confirming the financial transaction or deal, contracts confirming the conclusion of transactions, or other legally binding documents relating to the execution of financial transactions and/or the conclusion of transactions, immediately, but no later than within 3 working days of the execution of the financial transaction or the conclusion of the transaction.

12.2. The Company must maintain records of customers with whom transactions or business relationships have been terminated under the circumstances specified in clause 3.8 of the Policy or other circumstances related to breaches of the anti-money laundering and/or counter-terrorist financing procedures (Appendix No. 2). Data shall be entered into the register in chronological order no later than within 3 working days of the occurrence or discovery of the specified circumstances.

12.3. Data from the registration logs shall be retained for 8 years from the date of the conclusion of transactions or business relations with the customer.

12.4. Copies of documents confirming the customer's identity, details of the beneficiary's identity, other data obtained during the customer identification process, and documents relating to accounts and/or contracts (original documents or documents in electronic form, reports stored in electronic form in accordance with the Procedure for the Selection of Paper Documents and their Storage in Electronic Form) must be retained for 8 years from the date of the conclusion of transactions or business relations with the customer.

12.5. Correspondence relating to business relations with the client must be retained for 5 years from the date of the conclusion of the transactions or business relations with the client, on paper or in electronic form.

12.6. Retention periods may be extended for a further period of no more than 2 years where there is a reasoned instruction from the competent authority.

12.7. Documents confirming a financial transaction or transaction, or other legally binding documents relating to the execution of financial transactions or the conclusion of transactions, must be retained for 8 years from the date of the financial transaction or the conclusion of the transaction.

12.8. Employees are prohibited from informing the customer or other persons that information regarding the customer's financial transactions or concluded transactions, or the investigation conducted in relation thereto, has been submitted to the FNTT.

13. FUNCTIONS AND RESPONSIBILITIES OF THE RESPONSIBLE PERSON

13.1. The Company's director shall, by his or her decision, appoint a Responsible Person for the prevention of money laundering and terrorism financing, who shall implement the measures for the prevention of money laundering and/or the financing of terrorism set out in the Policy. In the event that the Company's director does not appoint a Responsible Person or the Responsible Person is unable to perform their functions, the Company's director shall be deemed to be the Responsible Person.

13.2. The Responsible Person's duties include:

13.2.1. maintaining records and ensuring data security;

13.2.2. assessing and managing the risks associated with the Company's Anti-Money Laundering and Counter-Terrorist Financing Policy across all its activities;

13.2.3. suspending suspicious financial transactions;

13.2.4. the implementation, review and updating of measures to prevent money laundering and terrorist financing;

13.2.5. cooperation and communication with the FNTT and other supervisory authorities on matters relating to the prevention of money laundering and/or terrorist financing;

13.2.6. familiarising the Company's employees with this Policy;

13.2.7. organising periodic training sessions on the prevention of money laundering and (or) terrorist financing for the Company's employees.

13.3. Before appointing a Responsible Person, the Company's manager assesses their competence, work experience and qualifications in the field of money laundering and terrorist financing, their level and nature of education, professional development, the nature and duration of their professional activities or work experience, and other factors that may influence the person's competence. The head of the Company shall ensure that the Responsible Person's functions are properly segregated to avoid conflicts of interest that increase or may increase the risk of money laundering and terrorist financing.

13.4. The responsible person shall have the right to receive and access all information necessary for the performance of their duties, including access to all information relating to customers, their representatives and beneficiaries, and to information regarding all financial transactions carried out by the Company and its customers.

13.5. The responsible person shall ensure that, upon receipt of a request from the FNTT, the information requested is provided immediately, but no later than within 14 working days of receipt of the request (in cases where the PPTFPĮ sets shorter deadlines for providing information to the FNTT, such information must be provided within those shorter deadlines)

13.6. The responsible person shall ensure that the Policy and other Company measures for the prevention of money laundering and terrorist financing are reviewed at least once a year and updated as necessary.

13.7. The responsible person shall periodically, but at least once a year, submit a report on the implementation of anti-money laundering and counter-terrorist financing measures to the Company's director, providing information on at least:

13.7.1. Money laundering and terrorist financing risk management, which includes:

13.7.1.1. The money laundering and terrorist financing risks faced by the Company and changes in their level;

13.7.1.2. The anti-money laundering and counter-terrorist financing risk management measures implemented;

13.7.1.3. proposals for amendments to the measures necessary for the effective management (mitigation) of money laundering and terrorist financing risks;

13.7.1.4. information on breaches identified during the implementation of internal control procedures and policies in the area of money laundering and terrorist financing prevention;

13.7.1.5. a report on how the Company complies with the requirements and obligations relating to the prevention of money laundering and terrorist financing.

13.8. If Company employees suspect that a Financial Transaction may be suspicious or discover other possible signs of money laundering and/or terrorist financing, they must immediately inform the Responsible Person.

13. FINAL PROVISIONS

14.1. Employees who breach the requirements of the Policy and the legislation referred to in clause 1.2 of the Policy shall be liable in accordance with the law.

14.2. All Company employees to whom this Policy may be relevant must be made aware of it and must comply with it.

14.3. This Policy is approved by the Company's Director. This Policy may be repealed, amended or supplemented only by a decision of the Company's Director. The Policy or any amendments thereto shall come into force on the date of the Company's Director's decision, unless the Director's decision specifies a different date of entry into force.

15. APPENDICES

15.1. Appendix No. 1 – Client questionnaire.

15.2. Appendix No. 2 – Simplified Client Questionnaire