POLICY ON PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

1. General

1.1. The Policy on Prevention of Money Laundering and/or Terrorist Financing (the **Policy)** of Corporate Services, UAB (the **Company)** establish rules that must be adhered to by the Company in order to properly manage risks of money laundering and/or terrorist financing.

1.2. The Policy intends to establish the following:

1.2.1. Governance in relation to management of ML/TF risks;

1.2.2. Principles regarding assessment of business-wide ML/TF risks to which the Company is exposed;

1.2.3. Principles, rules and responsibilities and processes to identify, manage and control ML/TF risks within the Company;

1.2.4. Requirements regarding identifying the Client and the beneficiary;

1.2.5. Requirements regarding assessment of the Clients' risk;

1.2.6. Requirements regarding performance of ODD, including, but not limited to, monitoring of Clients' transactions;

1.2.7. Principles regarding identification of suspicious transactions;

1.2.8. Requirements regarding filing SARs to the FIU (FNTT);

1.2.9. Requirements regarding maintenance of registration logs;

1.2.10. Requirements regarding storage of information;

1.2.11. Requirement regarding staff training; and

1.2.12. Principles regarding internal control.

1.3. The Company's approach to ML/TF prevention is based on the following core principles:

1.3.1. The Company opposes the crimes of ML/TF and will take all reasonable precautions to ensure that the Company's products and services are only utilised for legitimate purposes;

1.3.2. The Company will avoid relationships with those who the Company reasonably assesses as posing an unacceptable risk of ML/TF;

1.3.3. The Company's employees will undertake appropriate AML/CTF training (as defined in Company's *Corporate training policy* and *AML-CTF-Sanctions training procedure)*, so they understand the Company's AML/CTF obligations and to conduct their duties diligently to minimise AML/CTF risks;

1.3.4. The Company will not tolerate conduct from its employees which compromises the Company's compliance with AML/CTF requirements;

1.3.5. The Company will constantly monitor, measure and develop the Policy to ensure it is as effective as possible for the Company's business; and

1.3.6. The Company will manage changes to the products, business processes and systems to ensure ML/TF risks are identified and appropriately managed.

1.4. The Company recognises that AML/CTF compliance is an ongoing obligation which will require the Policy to undergo constant development to manage changes to the Company's operational environment and the risks of facilitating ML/TF to which the Company may be exposed.

1.5. When dealing with the Clients, the Company follows the following standards:

1.5.1. The Company should only deal with those Clients or conduct only those transactions that are acceptable to the Company;

1.5.2. The Company identifies the Clients, monitors their transactions, and takes steps to mitigate the risk of the Company's business being used for ML/TF;

1.5.3. The Clients' transactions must be monitored to ensure that the activity is within exceptions compared to the KYC data and previous activity and that the Company maintains the risk assessment of each Client and based on that risk level assesses proper EDD and sets time frames for the periodic update;

1.5.4. The Money Laundering Reporting Officer receives reports of suspicious activity, i.e. escalations (Annex 2);

1.5.5. The Company's employees are trained to recognize suspicious activities and to know what they should do if they suspect that a Client is attempting to launder funds or is involved in the financing of terrorism, including submitting reports of suspicious activity, i.e. escalations to the Money Laundering Reporting Officer;

1.5.6. The records on the Clients and transactions must be kept as required by the Policy.

1.6. The consequence of contravening regulations or failing to comply can be significant and include disciplinary measures, fines or both under local laws as well as the loss of reputation for the Company. The total execution of AML/CTF measures set forth in the Policy will help the Company and its employees to protect from the below:

1.6.1. **Reputational risk:** the reputation of a business is usually at the core of its success. The ability to attract good employees, Clients, funding and business is dependent on reputation. Even if a business is otherwise doing all the right things, if the Clients are permitted to undertake illegal transactions through that business, its reputation could be irreparably damaged. A strong AML / CTF program helps to prevent a business from being used as a vehicle for illegal activities;

1.6.2. **Operational risk:** this is the risk of direct or indirect loss from faulty or failed internal processes, management and systems. In today's competitive environment, operational excellence is critical for competitive advantage. If AML/CTF program is faulty or poorly implemented, then operational resources are wasted, there is an increased chance of being used by criminals for illegal purposes, time and money is then spent on legal and investigative actions and the business can be viewed as operationally unsound;

1.6.3. **Legal risk:** if a business is used as a vehicle for illegal activity by its Clients, it faces the risk of fines, penalties, injunctions and even forced discontinuance of operations;

1.6.4. **Financial risk:** if a business does not adequately identify and verify Clients, it may run the risk of unwittingly allowing a Client to pose as someone they are not. The consequences of this may be far reaching.

1.7. **The Policy is based on the following legal acts**:

1.7.1. The Law on Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania (No VIII-275, as of 19 June 1997 with all its later amendments and updates);

1.7.2. The Law on Implementation of economic and other financial sanctions of the Republic of Lithuania (No IX-2160, as of 22 April 2004 with all its later amendments and updates);

1.7.3. Code of Criminal Procedure of the Republic of Lithuania (No VIII-1968, as of 29 September 2000 with all its later amendments and updates);

1.7.4. Procedure on Suspension of Suspected Money Operations or Transactions and Submission of Information regarding Suspicious Money Operations or Transactions to the Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania approved by the Order No 1V-701 of the Minister on the Interior of the Republic of Lithuania as of 16 October 2017 (with all its later amendments and updates);

1.7.5. Procedure on Managing of Registration Logs of Monetary Operations, Transactions and Clients approved by the Order No V-129 of the Director of the Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania as of 4 September 2017 (with all its later amendments and updates);

1.7.6. Order on Technical Requirements for the Client Identification Process for Remote Identification Using Electronic Means of Direct Video Transmission Clients approved by the Order No V-314 of the Director of the Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania as of 30 November 2016 (with all its later amendments and updates);

1.7.7. List of Criteria for Possible Money Laundering and identification of suspicious money operations or transactions approved by the Order No V-240 of the Director of the Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania as of 5 December 2014 (with all its later amendments and updates);

1.7.8. Instructions for Supervision of the Proper Implementation of International Financial Sanctions by the Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania in the Field of Regulation approved by the Order No V-273 of the Director of the Financial Crime Investigation Service under the

Ministry of the Interior of the Republic of Lithuania as of 20 October 2016 (with all its later amendments and updates);

1.7.9. Order V-129 on Approval of Information Provided in Accordance with the Requirements of the Law on Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania Approval Form for Submission approved by the Director of the Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania as of 21 May 2015 (with all its later amendments and updates);

1.7.10. Criteria for possible terrorist financing issued by the State Security Department of the Republic of Lithuania as of 22 December 2015 (with all its later amendments and updates);

1.7.11. Guidelines for Financial Market Participants to Prevent Money Laundering and/or Terrorist Financing approved by the Resolution No 03-17 of the Board of the Bank of Lithuania as of 12 February 2015 (with all its later amendments and updates); and

1.7.12. Other legal acts that are not indicated in the above list.

2. Definitions

2.1. The following words when used in this Policy shall have the below meaning:

2.1.1. **Assets** shall have the meaning of objects, funds, securities, other financial instruments, other assets and property rights, results of intellectual activity, information, actions and results of activities, other property and non-property values, as well as any other physical or non-physical, movable or immovable property, tangible or intangible assets and legal documents or instruments in any form, including electronic or digital, evidencing title to or rights to these assets;

2.1.2. **Beneficiary** shall have the meaning set forth in Art. 5.8.2 of this Policy;

2.1.3. **Business day** shall have the meaning any day other than Saturday, Sunday or public holiday in the Republic of Lithuania;

2.1.4. **Business relationship** shall have the meaning of business, professional or commercial relationship between the Company and the Client which is related to the Company's professional activities and which was intended to continue for a certain period at the time of establishing the relationship. The Company enters into business relationships by opening payment account for the Client;

2.1.5. **Correspondent relations** shall have the meaning of:

2.1.5.1. banking services provided by one bank (correspondent) to another bank (respondent), including the provision of current or other liability accounts and related services such as money management, international money transfers, check clearing, transferable accounts and foreign exchange;

2.1.5.2. relationships between financial institutions, including where the correspondent institution provides similar services to the respondent institution, and relationships established for the purpose of securities transactions or transfers of funds.

2.1.6. **Client** shall have the meaning of a person to whom the Company provides its services. Unless otherwise specified in this Policy, the Client shall mean both a natural person (Client) and a legal person (Client legal person);

2.1.7. **Close associate** shall have the meaning set forth in Art. 5.11.5 of this Policy;

2.1.8. **Company** shall have the meaning of Corporate Services, UAB, a limited liability company organized and existing under the laws of the Republic of Lithuania, data about the company kept with the Companies' Register of the Republic of Lithuania, company code 304630394, having its registered office at Kuosų g. 9-87, Vilnius, Lithuania and holding unlimited electronic money institution license No 51 issued by the Lithuanian financial supervisory authority Bank of Lithuania as of 5 March 2019;

2.1.9. **Client legal person** shall have the meaning of a legal person to whom the Company provides its services. Any foreign organization recognized as a legal person under the Lithuanian law or the laws of a foreign state is also considered a legal person.

2.1.10. **Client** shall have the meaning of a natural person to whom the Company provides its services;

2.1.11. **EU member state** shall have the meaning of European Union member state European Economic Area member state;

2.1.12. **FIU (FNTT)** shall have the meaning of the Financial Crime Investigation Services under the Ministry of Interior of the Republic of Lithuania;

2.1.13. **ID** shall have meaning of: (a) passport; (b) identity card; or (c) driver's license issued in EEA complying with the requirements set forth in the Directive 2006/126/EC of the European Parliament and of the Council as of 20 December 2006 on driving licenses (recast);

2.1.14. **Immediate family members** shall have the meaning set forth in Art. 5.11.4 of this Policy;

2.1.15. **ML** shall have the meaning of money laundering which is defined as:

2.1.15.1. **Placement,** i.e. changing the legal status of the assets or transferring the assets knowing that the assets is derived from or participating in a criminal activity in order to conceal or disguise the illegal origin of the assets or to assist any person involved in the criminal offense to avoid the legal consequences of that criminal activity;

2.1.15.2. **Layering,** i.e. concealment or disguise of the true nature, true origin, source, location, disposition, movement, ownership or other rights with respect to assets, knowing that such assets is derived from or participating in a criminal activity;

2.1.15.3. **Integration,** i.e. acquisition, management or use of assets, knowing at the time of acquisition (transfer) that the assets was obtained from or participating in a criminal activity;

2.1.15.4. Preparation, an attempt to commit, complicity in committing any of the acts specified in Arts. 2.1.13.1 - 2.1.13.3 of this Policy.

For more detailed explanation, refer to Annex 1.

2.1.16. **Law** shall have the meaning of the Law on Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania (No VIII-275, as of 19 June 1997 with all its later updates and amendments);

2.1.17. **Politically exposed persons (PEPs)** shall have the meaning of natural persons entrusted with prominent public functions, their close associates and immediate family members;

2.1.18. **Policy** shall have the meaning of this document;

2.1.19. **Prominent public functions** shall have the meaning set forth in Art. 5.11.3 of this Policy;

2.1.20. **Related transactions** shall have the meaning of several transactions that are considered to be related to each other if the Client:

2.1.20.1. Executes several deposit transactions to the Client's payment account per day (24 hours), the aggregated amount of which is equal to or exceeds €15,000 or the equivalent amount in foreign currency;

2.1.20.2. Executes several withdrawal transactions to the Client's payment account per day (24 hours), the aggregated amount of which is equal to or exceeds €15,000 or the equivalent amount in foreign currency;

2.1.20.3. Executes other transactions per day (24 hours), which according to the data available to the Company, are interrelated and the aggregated amount of which is equal to or exceeds €15,000 or the equivalent amount in foreign currency;

2.1.21. **Senior manager** shall have the meaning of the Company's senior official or employee who has sufficient knowledge of ML/TF risks that the Company is exposed to and is responsible for making decisions that may affect the emerging risk;

2.1.22. **Suspicious transaction** shall have the meaning of a transaction involving assets which is suspected of being derived directly or indirectly from or participating in criminal activities offense and/or which is suspected of involving terrorist financing;

2.1.23. **TF** shall have the meaning of terrorist financing; an act considered a crime under Art. 2 of the International Convention for the Suppression of the Financing of Terrorist as of 9 December 1999;

2.1.24. **Transaction** shall have the meaning of any payment, transfer or receipt of funds;

2.2. Other terms not specified in this Policy shall have the meaning prescribed to them in the Law.

3. Governance

3.1. The Company's management is aware of the importance of the prevention of ML/TF and that effective prevention of ML/TF requires an ongoing investment of time, effort, funds and human resources. The Company's management must avoid situations where *everyone is responsible* but actually *no one is responsible.* The Company's management ensures that the AML/CTF functions are not self-assigned, the importance of the AML/CTF is not underestimated, and the AML/CTF is not performed in a formal way. The Company's management stresses the importance of the AML/CTF, educates the employees and provides respective resources to ensure proper prevention of ML/TF.

3.2. The Company's management creates corporate culture that stresses the importance of prevention of ML/TF and is led by an example. To achieve that, the Company shall ensure that there is a sufficient number of employees in the Company's AML unit and that all employees are assigned with certain functions. The assignment of the authority and responsibilities are clearly communicated and made in writing. Each employee in the Company's AML positions is presented with job description that clearly defines respective employee's functions and tasks.

3.3. Applicants to the Company's AML positions are screened with background and reference checks before a job offer is extended. Prevention of ML/TF is the core participant (and responsible personnel) in the Company's operations. Therefore, in relation to the foregoing, the Company must ensure that employees in the Company's AML positions possess sufficient knowledge, skills and experience in relation to their assigned functions. If necessary, the expertise may be checked with relevant tests. All of the foregoing must be documented in writing.

3.4. All employees have regular meeting with the Company's management regarding their performance. Such meetings are documented in writing. The Company ensures that employees' skills remain up to date by providing continuous training and evaluation (for the performance of the such employee's functions). The Company's management must ensure that all employees are treated equally irrespective of their position and title, and culture of integrity, honesty and respect is maintained in the Company.

3.5. The Company's Management Board shall be accountable to adopt required internal policies and procedures to ensure prevention of ML/TF and to set and oversee adequate and effective internal controls in relation thereto.

3.6. The Company must ensure that all times the Company is allocated with the sufficient resources to perform the prevention of ML/TF properly at every organizational level. The available resources must correspond to the Company's AML risk assessment, i.e. to the risk level the Company is exposed to.

3.7. Member of the Company's Management Board shall be appointed as a responsible person to ensure proper implementation of prevention of ML/TF in accordance with the Law and other applicable legal acts intended to ensure prevention of ML/TF. Appointment of such member of the Company's Management Board must be reported to the FIU within 7 (seven) business days following such appointment.

3.8. In addition to the member of the Management Board responsible person to ensure proper implementation of prevention of ML/TF in accordance with the Law and other applicable legal acts, the Company shall appoint a Money Laundering Reporting Officer (the **MLRO)** who shall be responsible for conduction of communication with the FIU (FNTT). Appointment of the MLRO must be reported to the FIU (FNTT) within 7 (seven) business days following such appointment.

3.9. The Money Laundering Reporting Officer shall be responsible for implementation of this Policy. The Money Laundering Reporting Officer shall periodically, however at least once a year, report to the Management Board on performance of the overall AML/CTF in the Company. Such report shall be made in writing, completing a form approved by the Company's Management Board.

4. AML Risk assessment and risk-based approach

4.1. To ensure effective management of the ML/TF risks, the Company must perform a business-wide ML/TF risk assessment. The risk assessment shall help the Company to understand any emerging ML/TF risks and assess to which areas the Company must allocate more resources when applying AML/CTF measures.

4.2. The Company shall ensure that the business-wide ML/TF risk assessment is performed, revised and updated regularly, at least once a year and/or upon any significant change.

4.3. Prior to starting to provide a **new financial service (product) or before starting to provide an existing financial service (product) to a new Client segment** (e.g. Clients operating in a new industry that Company has not yet encountered with), in a new geographical area or through a new delivery channel, the Company shall assess related ML/TF risks. The Company shall also assess the ML/TF-related risks associated to business uses of new or developing technologies (both for new and existing services (products)). Adequate measures for managing the aforementioned risks shall be decided based on the results of the assessment of such service (product).

4.4. A **business-wide risk assessment** must be proportionate to the nature and size of activities carried out by the Company and its products/services shall be performed taking into account the risks inherent to the Company's activities and their factors, as well as the risks identified in the National ML/TF Risk Assessment of the Republic of Lithuania and the European Commission's ML/TF risk assessment.

4.5. The Company shall ensure that when carrying out the business-wide ML/TF risk assessment the Company relies on up-to-date and objective information. The Company's business-wide ML/TF risk assessment shall be based on data that would allow for the correct identification of the level of ML/TF risks (e.g. the risk assessment shall include various statistics, i.e. the number of the Company's Clients and their distribution by different risk groups; the number of the Client using high-risk products; the number (value) of payment transactions in high- risk countries; the number of Clients active in high-risk countries).

4.6. The Company must annually assess ML/TF risks that the Company is exposed to itself. At least the following risks shall be taken into consideration while assessing ML/TF risks that the Company is exposed to itself:

4.6.1. Clients' risk;

4.6.2. Products and/or services and/or operations risk;

4.6.3. Delivery channel risk;

4.6.4. Geographical risk; and

4.6.5. Conflict of interest risk.

4.7. The Company must also assess the risks of certain industries that its Clients operate in, if such industries are considered as to pose higher risk and certain specific means and measures are required to mitigate risks posed by such industries (e.g. cryptocurrency related activities).

4.8. All business-wide ML/TF risk assessments performed by the Company and subsequent amendments and/or updates relating to such risk assessments shall be documented. The Company's Management Board must be acknowledged with the results of the business-wide ML/TF risk assessment.

4.9. The report of the Company's business wide ML/TF risk assessment must contain at least the following information: (a) risks that the Company is exposed to; (b) factors affecting ML/TF risks; (c) the likelihood of such factors materialising; (d) their impact; and (e) the applied risk management (mitigation) measures.

4.10. Having performed the business-wide ML/TF risk assessment and established that the applied risk management (mitigation) measures are not sufficient, the Company shall prepare a risk management (mitigation) action plan that shall be approved by the Company's Management Board.

4.11. Assessment of the ML/TF risks that the Company is exposed to is performed in accordance with the Procedure of the Company's business-wide ML/TF risk assessment that determines at least the following:

4.11.1. the sources of information used for carrying out the Company's business-wide ML/TF risk assessment(s);

4.11.2. a data collection and evaluation process;

4.11.3. indicators identifying ML/TF risks, the likelihood of them emerging and their impact;

4.11.4. the duties and responsibilities of the Company' staff member responsible for the Company's business-wide ML/TF risk assessment;

4.11.5. a procedure for reporting the results of the Company's business-wide ML/TF risk assessment to the Company's Management Board and the Managing director (CEO);

4.11.6. the frequency of and a procedure for revising (updating) the Company's business-wide ML/TF risk assessment;

4.11.7. a procedure for preparing and implementing an action plan for managing (mitigating) any risks identified.

4.12. In addition to the above, the Company will aim to keep up to date with information that is published by various organisations in respect to ML/TF trends as such information may be useful in illustrating how various services have been used to facilitate ML/TF. The Money Laundering Reporting Officer will be responsible for ensuring the Policy is up to date and must recommend any proposed changes to reflect ML/TF trends

5. *How Know your Client* (KYC) is performed in the Company?

5.1. What is KYC?

5.1.1. KYC is an obligatory due diligence process in the Company performed in order to identify its Clients and ascertain relevant information pertinent to doing financial business with them. The main purpose of KYC process is to prevent identity theft, fraud, ML or TF.

5.1.2. The initial step of KYC process is to collect and document identification data about the Client and the Client's beneficiary (where relevant).

5.1.3. Client Due Diligence **(CDD)** is the second step of KYC process intended to verify the Client's identity and assess the risk, i.e. to obtain sufficient information on the Client in order to understand what is the nature and purpose of usage of the Company's services; what is the Client's activity, what is the source of funds (for clarity, source of funds shall not be mixed with source of wealth; i.e. source of funds is to be understood as the source of funds that shall arrive to Client's account, where source of wealth is to be understood as a manner/source how the Client overall gained its/his/her wealth), perform necessary checks, such as regarding status of politically exposed person, application of international financial sanctions and other restrictive measures, checking of adverse media etc. During CDD usually information regarding source of funds is obtained, however, obtaining of information should not be mixed with verification of information (i.e. collection of proof to verify the information provided by the Client). In certain cases, establishment of source of wealth may also be used, depending of the case by case situation, however, it is more common in EDD); in case of the Client legal person, to understand the organizational structure of the Client. CDD must not be seen as a process or a "checklist" exercise to simply collect Client's information.

5.1.4. In case during the CDD it is established that the Client possess higher ML/TF risk in accordance with the Company's internal procedure or certain circumstances that require application of enhanced due diligence (EDD) according to the applicable law are established, EDD must be applicable (refer to Art. 5.9 of the Policy)

5.1.5. Ongoing due diligence **(ODD)** is applicable via monitoring of the Client's operations and comparing them to the previously obtained data and performing periodic reviews of the Client.

5.1.6. Simplified due diligence **(SDD)** is a process where, under certain circumstances the law allows the company to deviate from the standard requirements of CDD.

5.1.7. This Policy further details performance of KYC (SDD, CDD, EDD and ODD).

5.2. Purpose of CDD

5.2.1. CDD refers to the minimum due diligence measures which must be performed at the start of each business relationship. Establishment of the Client's identity and of the beneficiary is the process of the collection and verification of the Client's information.

5.2.2. CDD measures include, but are not limited to:

5.2.2.1. Identification and verification of Client and beneficiary identity;

5.2.2.2. Understanding the Clients' ownership and control structure;

5.2.2.3. Obtaining and assessing information about the purpose and the expected use of the Company's products/services, typical expected activities;

5.2.2.4. Understanding the business activities of the Company's Clients;

5.2.2.5. Performing screening to identify any PEP or international financial sanctions and international restrictive measures exposure;

5.2.2.6. Performing Client risk assessment and risk scoring (according to the requirements laid out in *Customer Risk Assessment Procedure)* to determine Client risk classification.

5.2.3. CDD shall provide the Company with knowledge about its Clients, including understanding of the purpose and intended nature of the business relationships. Based on information obtained from the Client, the Company shall not only assess the risks associated with the Client but shall also use (rely on) such information during the later stages of the business relationship with the Client, e.g. when conducting ODD of the business relationships and the Client's transactions and assessing whether the transactions performed by the Client are consistent with the Company's knowledge of the Client and the Client's activities, source of funds and whether the Client meet the criteria for possible suspicious transactions that could help uncover activities associated with ML/TF.

5.3. Performance of CDD

5.3.1. CDD must be performed in the following cases:

5.3.1.1. Before establishment of the business relationship with the Client;

5.3.1.2. While executing and accepting money transfers in accordance with the 2015 May 20 Regulation (EU) 2015/847 of the European Parliament and of the Council on information to be provided on transfers of funds and repealing Regulation (EC) No 1060/2009 1781/2006;

5.3.1.3. When there are doubts regarding authenticity and accuracy of the data previously obtained on the Client or the beneficiary;

5.3.1.4. In any other case when there is a suspicion that ML and/or TF activities were, are or will be performed.

5.3.2. The Company must perform CDD not only to the new but also to the existing Clients (i.e. periodic review), when the Company becomes aware of the **new circumstances or information in relation to any of following**:

5.3.2.1. the risk assigned to the Client,

5.3.2.2. the identity of the Client and/or beneficiary;

5.3.2.3. activities of the Client and/or beneficiary;

5.3.2.4. other significant issues related to the Client;

5.3.2.5. when there is an obligation to provide information in accordance with Article 2 of the Resolution of the Government of the Republic of Lithuania No. 1017 as of 23 September 2015 regarding implementation of the Council Directive 2011/16/EU on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC and the implementation of international agreements and arrangements of the Republic of Lithuania on the automatic exchange of information on financial accounts.

5.3.3. While performing the CDD, the Company shall:

5.3.3.1. identify the Client and verify the information obtained during the due diligence process, relying on documents, data or information received from a

reliable and independent source. Data, documents or information obtained from a reliable and independent source shall include official documents with the person's photograph and/or relevant registration number that cannot be easily copied or falsified (a passport, an identity card, a legal person's registration certificate, an extract from the Companies' Register, notarised copies of documents, etc.), specifying the Client's full name, personal identification number or another unique combination of characters assigned to the person for identification purposes, their nationality (where relevant), the person's photograph and/or signature, etc. (for natural persons) or the name, address, code, number of the registration certificate, VAT number, etc. (for legal persons) and information from reliable publicly available databases;

5.3.3.2. identify the Client's beneficiary and apply measures needed for verifying the beneficiary's identity to establish who the beneficiary is;

5.3.3.3. identify the Client's representative where the Client acts through a representative;

5.3.3.4. establish whether the Client acts on its own behalf or is under someone's control;

5.3.3.5. establish whether the Client, the Client's representative and the beneficiary are politically exposed persons;

5.3.3.6. assess whether there are any grounds for enhanced Client due diligence and enhanced monitoring of the business relationships;

5.3.3.7. assess the purpose and intended nature of the business relationships;

5.3.3.8. verify if the Client, the Client's representative and the beneficiary are not included in the list of persons who are subject to international financial sanctions and other restrictive measures;

5.3.3.9. conduct ongoing monitoring of business relationship and transactions, including investigations of transactions, with a view to ensuring that the transactions performed are consistent with the Company's information on the Client, the Client's business and risk profile, including information on the source of funds;

5.3.4. The Company must perform CDD against actual data, documents and information. In addition, it must be ensured that at any time of its activities the Company holds available actual data in relation to its Clients. For the purpose of the foregoing requirement, (a) data, documents and information submitted or obtained by the Company must not be older than 3 (three) months old at the moment of their submission; and (b) data, documents and information on the Client must be periodically renewed or any time the Company becomes

aware that there were changes in relation to the Client and the Company is aware or cannot be unaware of such changes.

5.4. Remote CDD

5.4.1. CDD in the Company is only performed in a remote manner via direct image transmission method and the use of qualified electronic signature to confirm information about the Client's identity.

5.4.2. While performing remote CDD via direct image transmission method, the following must be performed:

5.4.2.1. Image of the Client's face is captured and transmitted directly. The face in the image must be clear and be outstanding from the surrounding;

5.4.2.2. Image of the Client's ID is captured and transmitted directly. (A) If the Client presents his/her ID card or driving license, then both sides of the ID card must be captured; (B) if the Client presents his/her passport, then only the page with the Client's photo must be captured.

5.4.3. While performing remote CDD via the use of qualified electronic signature to confirm information about the Client's identity, the following must be performed:

5.4.3.1. Image of the Client's ID is captured and transmitted directly. (A) If the Client presents his/her ID card or driving license, then both sides of the ID card must be captured; (B) if the Client presents his/her passport, then only the page with the Client's photo must be captured.

5.4.3.2. The Client must confirm the ID is there own by the use of a qualified electronic signature which conforms to the requirements of Regulation (EU) No 910/2014. Qualified electronic signatures from third countries supported by a qualified certificate for electronic signature shall be recognised under Article 14 of Regulation (EU) No 910/2014; e.g. SmartID

5.4.3.3. The Client may be provided with additional instructions, e.g. to change the position of his/her face or ID document, to remove the head or face cover, glasses or other objects that interfere with the proper capture of the Client's facial image.

5.4.3.4. After the above actions are performed, the Client shall be informed that by submitting the data, the Client also confirms the accuracy of such data.

5.4.4. Actions indicated above shall be performed continuously and shall be part of the single Client identification process, i.e. it may not be interrupted. Special programs, applications or other tools must be used to ensure that the process of taking photos is uninterrupted and that the transfer of the images in possible in real time only. If interrupted, the process must be restarted. Only one person may participate in a single process of the remote CDD.

5.4.5. The directly transmitted images must be of such quality that the information can be easily read from the submitted ID documents and in case of direct image transmission the characteristics of the Client and the person depicted in the ID document can be clearly seen and that there would no doubt that the picture in the submitted ID document is of the person participating in the remote CDD. The Company must ensure that the data captured in the images may not be altered or used in any other manner that is not compatible with the CDD.

5.4.6. The remote CDD must be discontinued in case if there is one of the following:

5.4.6.1. the image is not transmitted in real time;

5.4.6.2. direct transmission of the images is interrupted or there are problems with direct transmission of the images;

5.4.6.3. the quality of the images does not allow to accurately see the Client's face and/or to establish the Client's identity from the facial image of the ID document in case of direct image transmission;

5.4.6.4. the Client's ID document is not recorded in compliance with all requirements (i.e. not both sides of ID card is captured etc.);

5.4.6.5. the Client fails to perform the actions requested by the Company;

5.4.6.6. it is established that the ID document provided by the Client is damaged, forged or there are other indications that would cast doubt on the authenticity of such ID document (e.g., a copy of the ID document is displayed). In such a case, the Client identification process may be continued and the information necessary to identify the Client and the beneficiary shall be collected only for the purpose of immediately notifying the FIU of such cases after assessing the risk of ML/TF;

5.4.6.7. it is established that the ID document submitted by the Client does not comply with the information content requirements for such a document;

5.4.6.8. the Company has reasonable doubts that the Client to be identified and the owner of the submitted ID document is not the same person;

5.4.6.9. more than one person is involved in the Client direct image transmission identification process. For clarity, if the Company fails to identify another person during the remote CDD and therefore, to discontinue the remote CDD, it shall be considered that the Company failed to comply with the requirement of the Law requesting to establish whether the Client is acting on his/her own. However, each situation must be treated on case by case basis and it must be assessed whether the person visible during remote CDD process has control over the Client or in case of direct image transmission is that an accidental appearance of the person, e.g. the person passes by in the back and that is clearly unrelated to the remote CDD;

5.4.6.10. the person does not consent to the direct transmission of the photo;

5.4.6.11. the Client and the Company are unable to communicate or understand each other for different languages or other reasons.

5.4.7. The Company having assessed the threat of ML/TF, shall have the right to suspend and terminate the remote CDD process due to circumstances other than those indicated in Art. 5.4.4 of the Policy.

5.4.8. The Company may not extend or resume an interrupted remote CDD process and remote CDD shall be possible only upon the commencement of a new identification process complying with the requirements indicated above.

5.4.9. The Company shall be entitled establish additional security or technical requirements for proper and safe remote CDD.

5.4.10. The images captured during remote CDD and stored by the Company must have a tag indicating the Client's name, last name, personal code, IP address (if the Client uses computer for the identification process), from which the Client applied for his/her identification, and the date the images were captured.

5.4.11. The Company must ensure the security of the personal data intended for remote CDD, protection of the Client's data from accidental or illegal destruction, alteration, disclosure, as well as from any other illegal processing, in accordance with the requirements of the law applicable in relation to processing of the Client's personal data.

5.4.12. The Company must train its employees to properly perform remote CDD and use tools that the Company has purchased for the foregoing purpose and must ensure that the employees are familiar with the requirements regarding remote CDD.

5.5. Data to be obtained on a Client natural person during CDD

5.5.1. When performing CDD for the Client the following data should be obtained and verified:

5.5.1.1. First name, last name

5.5.1.2. Personal identification code when available (in other cases date of birth)

5.5.1.3. Client's photo;

5.5.1.4. Signature (except the cases when signature in not mandatory in ID); and

5.5.1.5. Citizenship, (except stateless person – then the state which issued the identity document, also in cases where it is optional on the identification document the customer must provide the data on their citizenship)

5.6. Data to be obtained on the Client legal person

5.6.1. When performing CDD for the Client legal person the following data should be obtained and verified:

5.6.1.1. Name;

5.6.1.2. Legal form;

5.6.1.3. Registered office address;

5.6.1.4. Address of the actual activities of the Client legal person;

5.6.1.5. Code, if given;

5.6.1.6. Certificate of Incorporation (for the Clients that are not able to provide the extract from the relevant register due to different legal system (such as common law)) or extract from the relevant register and date of its issuance.

5.6.2. The Company must also establish the identity of the representative(-s) of the Client legal person. When establishing the identity of the representative of the Client legal person, data indicated in Art. 5.5.1 of the Policy must be obtained.

5.6.3. The Company must also establish the ground of representation of the Client legal person. I.e., if the Client legal person is being represented by the director or other person that is entitled to represent the Customer legal person according to the Articles of Association of such Client legal person (or any other document to the same effect).

5.6.4. If the Client legal person is being represented by another person who is not entitled to represent the Client legal person in accordance with its statutory documents, a power of attorney must be obtained from such person. Before accepting such power of attorney, the Company must make sure of the following: (a) if the power of attorney is issued by a person entitled to do so (check for quantitative signing rule); (b) if there date of issuance and term of the power of attorney; (c) what action the representative can perform, i.e. if only to apply for the opening of the payment account or as well can have full access to payment account and manage it etc. (the representative should not be entitled to more rights than it is actually indicated in the power of attorney).

- If the power of attorney is issued outside of Lithuania, it must be notarized and apostilled.
- For clarity, each person that is entitled to access and manage (e.g. initiate and authorize payments) the payment account opened for the Client legal person by the Company shall be considered as the representative of such Client legal person. In the foregoing case the Company must: (a) request power of attorney (and respectively check it); and (b) establish the identity of such representative, i.e. obtain data indicated in Art. 5.5.1 of the Policy and screen with Ondato or any other IT solution intended for the same purpose. The Company must not allow access the Client's legal person payment account to any person whose identity has not been established and scope of authorization established.

5.6.5. If the Client legal person is being represented under the power of attorney, the Company must always obtain the following data on the director (may be referred as the CEO, managing director, president etc.) of the Client legal person: (a) name, last name; (b) personal code, if assigned or date of birth; (c) citizenship and obtain copy of ID document of the director.

5.6.6. Documents that the Company must obtain on the Client legal person shall be detailed in the Onboarding procedure.

5.7. Other information to be obtained during CDD

5.7.1. In addition to the information indicated in Arts. 5.5-5.6 of the Policy, information indicated below in Art. 5.7.2 must be collected in relation to each Client of the Company. Such information must be collected before the establishment of the business relationship and during the business relationship. The purpose of collecting such information is to get to know the Company's Client, i.e. to obtain information/data/documents based on which (a) the Client's risk level shall be assigned (taking into consideration other data as well); (b) the ODD (in form of on-going and retrospective monitoring and periodic review) shall be conducted.

5.7.2. While performing CDD, the Company must obtain sufficient information:

5.7.2.1. To understand the structural organization of the Client legal person;

5.7.2.2. To understand the Client's activities and to assess if the usage of the Company's services and/or products makes sense (to understand the nature and the purpose of using the Company's services). The Company must ensure that there are no discrepancies in the information provided by the Client and other information obtained by the Company regarding the Client's activities;

5.7.2.3. To understand how the intended product and/or services will be used, e.g. in case of payments where the payments will be sent, how often, monthly turnover etc. The collected information must be tailored to the Company's services and must serve as a basis for ODD;

5.7.2.4. To understand the source of funds and/or the source of wealth (in case of EDD). For clarity, understanding source of funds and/or the source of wealth means obtaining respective proof to validate the information provided by the Client;

5.7.2.5. To establish whether the Client (or it's beneficiary(-s), director(-s), representative(-)s) is not a politically exposed person as defined in the Law or international financial sanctions and international restrictive measures are applicable towards the Client.

5.7.3. The above list is not exhaustive. The Company tailors the scope of its performed KYC taking into consideration outcome of its ML/TF risk assessment and the services or products the Company offers. Also, KYC for the Clients that are considered to pose higher ML/TF risk is deeper and more thorough. I.e. the higher the Client's ML/TF risk, the more information and documents the Company must obtain as well as apply additional CDD measures and obtain additional information that would allow to know the Client and understand its business, sources of funds, origins of assets, ownership and control structure, etc.

5.7.4. Proper performance of the KYC is critical for further proper performance of ongoing and retrospective monitoring. The Company may only be able to notice any deviations in the Client's behaviour if the Company has sufficient data to make a comparison.

5.8. Establishment of identity of beneficiary

5.8.1. The Company must always establish the identity of the beneficiaries. Complex ownership structures may be used to disguise links to criminal activities, avoid tax obligations, may involve PEPs and sanctioned persons or jurisdictions.

5.8.2. In accordance with the Law, beneficiary shall be defined as a natural person who owns or controls a Client legal person or foreign state entity and/or a natural person on whom behalf a transaction or activity is carried out. The beneficiary shall be considered to be:

5.8.2.1. in a Client legal person:

a. a natural person who owns or controls, directly or indirectly, a sufficient percentage of the

shares or voting rights of that Client legal person, including through the management of

the bearer shares, except for public limited liability companies whose securities are traded on regulated markets governed by European Union law and regulatory requirements to disclose information about its activities, or equivalent international standards are applicable, or otherwise controlled. A natural person who owns 25% and one share or more than 25% of the Client's property is considered a direct owner. The natural person(- s) controlling the company or several companies that owns 25% and one share or more than 25% of the Client's ownership is considered to be the indirect owner(-s);

b. in the case of an identified Client legal person, a natural person in a senior management

position, if the person referred to in Art.5.8.2.1 (a) of the Policy has not been identified or if there are doubts that the identified person is the beneficiary;

5.8.2.2. in trusts - all of the following persons:

a) the trustor(-s);

b) the trustee(-s);

c) the custodian(-s), if any;

d) natural persons benefiting from a Client legal person or entity without legal personality, or, in so far as such persons have not yet been identified, persons whose interests are represented or are represented by that Client legal person or entity without legal personality;

e) any other natural person who effectively controls the trust, whether directly or indirectly through ownership or other means;

5.8.2.3. in a legal person administering and distributing funds, in an entity of a similar form to a trust - a natural person holding a position equivalent to the duties specified in Art. 5.8.2.2 of the Policy.

5.8.3. However, for the purpose of this Policy, a beneficiary may be considered each natural person that owns at least [25 %] twenty five percent) for the Client legal person that are assigned to high risk. For clarity, if there is no person that holds at least [25%] (twenty five percent) in the Client legal person's share capital, rule indicated in Art. 5

5.8.3.1. of this Policy shall be applicable.

5.8.4. The following data must be obtained and verified about each beneficiary:

5.8.4.1. First name;

5.8.4.2. Last name;

5.8.4.3. Personal identification code when available (in other cases date of birth); and

5.8.4.4. Citizenship.

5.8.5. In addition to above, the Company must obtain and upon the request of the FIU provide the following information:

5.8.5.1. Identification data of the Client's beneficiary;

5.8.5.2. Proof of checks of information provided by the Client in reliable and independent sources;

5.8.5.3. Data on the Client's legal person ownership and management structure. For clarity, in order to be able to submit such information when requested, the Company must understand the whole ownership structure, it must raise no doubts for the Company and must be based on the documents.

In relation to the management structure, the Company must understand who adopts major decisions in the Client legal person and depending on the information, must challenge its knowledge of the beneficiary. E.g. if a person identified having exclusive decisive power in the management structure (e.g. a veto right for all decisions or prior approval required for all decisions), it must be challenged if such person is not a beneficiary.

- In case there is a nominal beneficiary, the beneficiary must be identified, as well the documented arrangement between the nominal and actual beneficiary must be obtained.

5.8.6. While establishing the identity of the beneficiary, the Company must verify the obtained data against information from reliable and independent source. The Company shall be entitled to request the Client to indicate public sources from which the data on beneficiary may be verified.

5.8.7. For avoidance of any doubt, the beneficiary must be identified before the end of KYC. I.e., business relationship cannot be established with the Client before beneficiary is identified.

5.8.8. The data on the beneficiary (refer to Art. 5.8.4 of the Policy) shall be verified using electronic identification means issued in the European Union operating under high or sufficient level of security electronic identification schemes, or by a qualified electronic signature using a qualified electronic signature certificate in accordance with Regulation (EU) No 1095/2010. 910/2014, either by electronic means allowing direct video transmission or by signing a written document.

5.9. Performance of EDD

5.9.1. Enhanced due diligence (EDD) is performed in addition to CDD in the following cases:

5.9.1.1. when international correspondent relationship is established with the foreign financial institutions (any financial institution will be considered as foreign when established outside Lithuania) or cryptocurrency related institution;

5.9.1.2. Business relationship is established with politically exposed persons (PEPs);

5.9.1.3. Business relationship is established with the Clients who are either citizens or are residing or Clients legal person are established in high-risk jurisdictions in accordance with the assessment of the European Commission;

5.9.1.4. Following risk assessment of the Client according to the requirements laid out in *Customer Risk Assessment Procedure),* EDD may be not applicable to the branch or subsidiary of the financial institutions or other obliged entities established in the European Union in which they have a majority shareholding and which are located in high risk third countries identified as such by the European Commission, provided that those branches or subsidiaries comply with established group requirements equivalent to the requirements of the Law;

5.9.1.5. Business relationship is established with the natural persons who are either citizens or are residing or Clients legal person are established in third countries identified as high risk in the lists of countries with serious deficiencies in the prevention of money laundering and/or terrorist financing published by the Financial Action Task Force (FATF) on Money Laundering and Terrorist Financing ;

5.9.1.6. higher risk of ML/TF is identified in accordance with the Company's risk assessment and management procedures.

5.9.2. While performing EDD in relation to establishment of the international correspondent relationship with foreign financial institutions or cryptocurrency related institution, the Company shall be obliged:

5.9.2.1. To gather sufficient information about the respondent institution in order to have a good understanding of the nature of its business and to determine the reputation and quality of supervision of the respective institution from publicly available information;

5.9.2.2. To assess the control mechanisms for the prevention of ML/TF of the financial institution receiving the funds;

5.9.2.3. To obtain the approval of the senior manager before establishing new correspondent relationship;

5.9.2.4. To document the respective liabilities of each financial institution;

5.9.2.5. To ensure that the responding institution has properly performed its Client identification (including verification of the Clients with direct access to the correspondent accounts, other Client identification activities) and, if necessary, may provide relevant Client identification data at the Company's request.

5.9.3. While performing EDD in relation to establishment of business relationship with the Clients who are PEPs, the Company shall be obliged:

5.9.3.1. To obtain the approval of the senior manager to establish business relations with such Clients or the approval to continue business relations with these Clients;

5.9.3.2. To take appropriate measures to determine the source of assets and funds related to the business relationship or transaction of such Client; and

5.9.3.3. To carry out enhanced ODD of business relationship with such Client.

The Company must ensure that it has proper internal control means to assure that the Company identifies PEPs in timely and proper manner.

5.9.4. While performing EDD in relation to establishment of business relationship with the Clients who are either citizens or are residing or Clients legal person are established in high-risk jurisdictions in accordance with the assessment of the European Commission, the Company shall be obliged:

5.9.4.1. To obtain additional information about the Client and the beneficiary;

5.9.4.2. To obtain additional information on the intended nature of the business relationship;

5.9.4.3. To obtain information on the source of funds and assets of the Client and the beneficiary;

5.9.4.4. To obtain information on the reasons for intended transactions;

5.9.4.5. To obtain the approval of the senior manager to establish business relations with these Clients or the approval to continue business relations with these Clients;

5.9.4.6. To carry out enhanced ODD of business relationship with such Client, increasing the number and terms of the applied control measures and selecting the types of transactions that will be further investigated;

5.9.4.7. To ensure that the Client's first payment is initiated from that Client's account opened with a credit institution where the credit institution is established in the EU Member State or in a third country with requirements equivalent to those laid down in the Law and supervised by the competent authorities.

- Based on the results of the National ML/TF risk assessment, the FIU may adopt additional measures to be applied to Clients (residents/citizens) and Client legal person established in a certain jurisdiction, such as:

5.9.4.8. Application of additional enhanced business relationship monitoring measures to reduce the risk of ML/TF;

5.9.4.9. Strengthening the reporting of suspicious transactions;

5.9.4.10. Restriction of business relationship or transactions with natural persons residing in high-risk third countries or Clients legal person established there by the European Commission.

5.9.5. While performing EDD in relation to establishment of business relationship or executing transactions with the Clients who are either citizens or are residing or Client legal person are established in countries included in the lists of countries with serious deficiencies in the prevention of and prevention of money laundering and/or terrorist financing published by the FATF, the Company must apply one or few additional measures and must (i.e. application of all measures indicated in Arts. 5.9.5.1-5.9.5.3 is obligatory, and in addition at least one additional measure of the choice of the Company must be applied):

5.9.5.1. To obtain the approval of the senior manager to establish business relations with these Clients or the approval to continue business relations with these Clients;

5.9.5.2. To take appropriate measures to determine the source of assets and funds related to the business relationship or transaction of such Client; and

5.9.5.3. To carry out enhanced ODD of business relationship with such Client.

5.9.6. While performing EDD in relation to Clients posing higher ML/TF risk according to the Company's internal procedures, the Company must apply one or few additional measures and must (i.e. application of all measures indicated in Arts. 5.9.6.1-5.9.6.3 is obligatory, and in addition at least one additional measure of the choice of the Company must be applied):

5.9.6.1. To obtain the approval of the senior manager to establish business relations with these Clients or the approval to continue business relations with these Clients;

5.9.6.2. To take appropriate measures to determine the source of assets and funds related to the business relationship or transaction of such Client; and

5.9.6.3. To carry out enhanced ODD of business relationship with such Client.

- If during the business relationship with Client, the Client's risk is levelled to high risk, the Company must perform EDD in relation to such Client immediately after the Company becomes aware of such change of risk.

5.9.7. Examples of such additional measures to be applicable may be e.g.: verification of source funds, collecting more information on the Client's business activities, collecting additional information on the Client's beneficiaries, collecting information on the Client's counterparties, reviewing of the Client's internal procedures (where relevant), sample testing (where relevant), obtaining documents verifying the Client's statements etc. However, the foregoing measures are only examples, not an exhaustive list. More detailed information shall be provided in the Onboarding procedure.

5.9.8. Enhanced due diligence is detailed in the Company's Onboarding procedure.

5.10. Simplified Due Diligence

5.10.1. Simplified due diligence as describe in Lithuanian AML law allows for the company to deviate from the standard requirements of Customer Due Diligence (CDD) and to apply less stringent measures to identify the customer.

5.10.2. Simplified due diligence as commented by the Bank of Lithuania does not require that the company verify the customers provided data using any reliable or independent sources e.g. passport.

5.10.3. The company is only applying simplified due diligence on the natural persons using the company's Mily/Pusdienlaiks project. The company has assessed the risk of its Mily project and determined that the risk of money laundering and/or terrorist financing or other predicate offences is low to non-existent.

5.10.4. The customer's risk shall be automatically assessed as low unless there arise factors which disqualify the customer from passing SDD see section "*Simplified due diligence will be prohibited under the following circumstances:"*

5.10.5. The company will apply certain restrictions to accounts that have gone through simplified due diligence:

5.10.5.1. Customers may cumulatively deposit or withdraw a maximum of 1.000 EUR (one thousand) during a calendar year.

5.10.5.2. Allow withdrawals to an account only in the name of the customer which has passed simplified due diligence.

5.10.6. When performing simplified due diligence, the company will:

5.10.6.1. Require from the customer their full legal name(s) including surname(s)

5.10.6.2. Require from the customer their personal code or if the customer does not have a personal code, then their date of birth.

5.10.6.3. Perform a name check to determine if the client is not found to be a person of interest i.e. sanctioned individual etc.

5.10.6.4. Ask the customer for the intended purpose and nature of the business relationship.

5.10.6.5. Monitor the customers transactions for any suspicious monetary operations or transactions.

5.10.7. Simplified due diligence will be prohibited under the following circumstances:

5.10.7.1. Enhanced due diligence is determined to the required.

5.10.7.2. The customer has provided false or misleading information.

5.10.7.3. The customer wishes to deposit or withdrawal more than 1.000 EUR in a calendar year.

5.10.7.4. The customer wishes to allow withdrawals to an account in the name of another person.

5.10.7.5. In cases when the client is under any suspicion, or where the MLRO says not to perform SDD, or in case the client has had an STR filed on their activity.

5.11. Risk assessment

5.11.1. A risk-based approach refers to the assessment of the potential risk of ML/TF posed by the Company's (potential) Client and implementation of the measures to reduce or mitigate such risk. As a result, the Company shall allocate and prioritize resources according to where the most risk mitigation is required.

5.11.2. Individual risk assessment of Company's Clients is described in *Onboarding procedure* and its annex – *Client Risk Assessment procedure* (the **Procedure)** to carry out individual ML/TF risk assessments and assign Clients (both when entering into and in the course of ongoing business relationships) to risk groups (categories). The Company shall ensure that the **Procedure** for the individual ML/TF risk assessment is regularly revised and, updated when necessary, and that it defines at least the

risk identification criteria, risk factors, procedure for the assessment of the ML/TF risks associated with the Client and frequency of such assessments.

5.11.3. The Company shall recognize the following risks:

- According to the nature:
  - Client risk;
  - Geographical areas risk;
  - Product and services risk;
  - Delivery channel risk;
  - Other risks.

- According to the risk level, the customers are categorized as:
  - Low;
  - Medium;
  - High;
  - Unacceptable or prohibited (beyond risk appetite).

All Company's clients shall be assigned at least to the following risk levels: **low**, **medium**, **high** and **unacceptable**. The Company may differentiate certain risk levels into smaller, detailed groups, e.g. high risk and very high risk. This shall be indicated, if necessary, in the Procedure.

The Company's Clients will be assigned to risk groups (categories) based on various criteria, e.g. the country of registration, the type of activity, the actual place of business, the ownership and control structure of the Client who is a legal entity, the Client's place of residence, the beneficiary's nationality, the nature and size of the transactions performed, the products (services) used. The foregoing list is not exhaustive.

5.11.4. The Company shall ensure that the automated solutions implemented by the Company for the purpose to manage ML/TF risks allow to identify any factors that might increase risk associated with the Client and assign the Client to a relevant risk level.

5.11.5. The Company must assess risk of its Clients before establishment of business relationship and on ongoing basis according to its internal procedures and depending on the results of the initial Client risk assessment, i.e. to which level risk the Client was initially assigned (e.g. if the risk level assigned to the Client is high, risk re-assessment must be conducted more often).

5.11.6. The Client's risk assessment must be conducted in the following cases:

5.11.6.1. Before establishment of the business relationship with the Client;

5.11.6.2. On ongoing basis according to the initially assigned risk level;

5.11.6.3. If new service/product is provided to the existing Client (i.e. if the usage of such product/service by the Client might lead to an overall higher risk of the Client);

5.11.6.4. If the Company becomes aware of the new circumstances (irrespective of the manner and form such information obtained); such new

circumstances as well includes information obtained during internal investigations, recalls, external notification on suspected fraud;

5.11.6.5. There is a significant deviation in the Client's behaviour from the information that the Company's had obtained during KYC or during overall business relationship with the Client.

- The above list is not exhaustive and the Client's risk level may be re-assessed at any time the Company may see it necessary and fit.

5.11.7. While assessing the Client's risk, at least the following must be taken into consideration:

5.11.7.1. Client's features:

- Client's business relationship is conducted in unusual circumstances without an obvious economic or visible legitimate purpose;
- Client resides in a third country;
- Clients legal person or entities without legal person status commence activities of a personal asset management company;
- Client legal person has nominal shareholders or issued bearer shares;
- cash predominates in the Client's business;
- the ownership structure of the Client legal person appears unusual or excessively complex given the nature of the Client's activities;

5.11.7.2. the characteristics of the Client's product, service, transaction or service channel:

a) Private banking;

b) The product or transaction may facilitate anonymity;

c) The Client's business relationship or transaction is concluded or carried out without the Client's physical participation in cases other than those provided for in Article 11.1 of the Law;

d) Payments received from unknown or unrelated third parties;

e) The Client's product or business practice, including the service delivery mechanism, is new and new or evolving technologies are used in dealing with both new and existing products;

f) The Client's transactions involving oil, arms, precious metals, tobacco products, cultural artefacts and other objects of archaeological, historical, cultural and religious significance or of rare scientific value, as well as ivory and protected species;

5.11.7.3. features of the territory (jurisdiction):

a) significant non-compliance of the anti-money laundering and terrorist financing system with international requirements has been identified in the country on the basis of reports by the FATF;

b) based on data from governmental and universally recognized non-governmental organizations that monitor and assess the level of corruption, the country has a high level of corruption or other criminal activity;

c) international financial sanctions and international restrictive measures, embargoes or similar measures imposed on a state by, e.g., the European Union or the United Nations;

d) the state either supports terrorist activities, or terrorist organizations listed in the list of international terrorist organizations operate in the state.

5.11.8. The above list is not exhaustive, it is listed for example purposes only. The Company must pay particular attention to any risk of ML/TF that may arise from the use of any kind of products, products, other human performance, services or transactions in order to disguise the identity of the Client and/or beneficiary (prone to anonymity).

5.11.9. Thus, the Company shall adopt a detailed its Client's risk assessment Procedure taking into consideration results of the Company's business-wide ML/TF risk assessment, the features of its Clients (e.g. certain legal forms or complex legal structures, certain industries in which the Company's Clients operates pose inherently higher ML/TF risk etc.), products the Company delivers or services provides (seamless and fast internal, SEPA and international money transfers, prepaid debit card etc.), the delivery channel (the Company business is conducted with no physical presence; identity of the Clients is established via remote identification means etc.) and geographical connections (e.g. residing/operating, sending/receiving funds to or from higher risk countries shall pose higher ML/TF risk) and other circumstances that may have impact on the risk level assigned to the Client. The risk assessment must be tailored to the activities of the Company. The Company's senior management shall avoid the situation where the risk assessment shall be performed in a formal manner, only to formally comply with the applicable legal requirements. The Company must be able to clearly and coherently explain the model it chose for the assessment of its Clients' risk.

5.11.10. Company shall perform the following assessments:

- **individual risk assessment** of each Client before entering into business relations with the Client or in case Company becomes aware of certain circumstances indicating the possible change in the Client's risk group. Company must ensure that, in case required, the Client's risk group is duly updated, and the actions related thereto are performed taking into account information provided. Where Company uses automated systems to allocate overall risk scores to categorise business relationship adhering to the risk criteria and does not develop these in-house but purchases them from an external provider, it should understand how the system works and how it combines risk factors to achieve an overall risk score. Company must always be able to satisfy itself that the scores allocated reflect Company's understanding of ML/TF risk and it should be able to demonstrate this to the competent authority;

As part of the risk assessment, Company may decide to weigh factors differently depending on their relative importance. When weighing risk factors, Company shall follow these main principles:

- the weighing is not unduly influenced by just one factor;
- economic or profit considerations shall not influence the risk score;
- the weighing shall not lead to a situation where it is impossible for any business relationship to be classified as high risk;
- high ML risk can be overruled by Company's weighing only with sufficient arguments related to applicable internal controls or other mitigating factors. The provisions of the law regarding situations that always present a high money laundering risk cannot be overruled by the Company's weighting.

5.11.11. The Client's risk must be regularly reassessed to ensure that the Company understands what risk its Clients pose at all times and therefore, is able to address it properly and to apply relevant risk mitigation means and measures. Periodicity of the Client's risk re-assessment depends on the risk level assigned to the Client. In case of dormant accounts, the Client must be treated as a new Client.

5.11.12. The Company shall ensure that where there is significant information that might affect the Client's risk assessment, e.g. where information and data submitted for the Client due diligence has been renewed, where new significant information on the Client and its business becomes known to the Company, where the Client intends to use a new service or product, where the nature of the Client's business relationship or operations changes, or where the Client's transactions may appear suspicious, the Client's risk assessment shall be reviewed and, if necessary, updated.

5.11.13. Where an increased risk associated with the Client is identified, additional information from that Client shall be obtained, enhanced ongoing monitoring of the Client's business relationships shall be applied, and a reassessment of the ML/TF risks associated with the Client or application of other risk mitigating measures shall be considered.

5.11.14. Company's MLRO shall be responsible for the implementation of the ML/TF risk assessment process (both Company wide and individual) in the Company.

5.11.15. The Client's risk assessment is detailed in the Company's *Customer Risk Assessment procedure*.

5.11.16. Company shall keep risk assessments up to date and under review. All risk assessments shall be documented and kept in a written form.

5.12. Politically exposed persons

5.12.1. Persons who have, or have had, a high political profile, or hold or have held, public office, can present a higher ML/TF risk, as their position may increase their vulnerability to corruption.

5.12.2. In accordance with the Law, the PEPs are defined as natural persons who have or have been entrusted with prominent public functions and their close family members or close associates.

5.12.3. Prominent public functions are the following positions held in the Republic of Lithuania, European Union, international or foreign institutions:

5.12.3.1. Head of state, head of government, minister, vice minister or deputy minister, secretary of state, chancellor of parliament, government or ministry;

5.12.3.2. a member of parliament;

5.12.3.3. member of the supreme courts, constitutional courts or other supreme judicial institutions, the decisions of which may not be appealed;

5.12.3.4. the mayor of the municipality, the director of the municipal administration;

5.12.3.5. a member of the management body of the supreme audit and control institution or the chairman of the board of the central bank, his deputy or a member of the board of the central bank;

5.12.3.6. an ambassador, a temporary charge d'affaires, a commander of the Lithuanian Armed Forces, commanders of the Armed Forces and units, the Chief of the Defense Staff or an officer of a high- ranking armed force of foreign states;

5.12.3.7. a member of the management or supervisory body of a state enterprise, public limited company, private limited company shares of which or part of the shares conferring more than 1/2 of all votes at the general meeting of shareholders of these companies is owned by the state;

5.12.3.8. a member of the management or supervisory body of municipal enterprises, public limited company, private limited company, the shares of which or part of shares conferring more than 1/2 of all votes at the general meeting of these companies belong to the municipality and are considered large enterprises under the Law on Financial Reporting of Enterprises of the Republic of Lithuania;

5.12.3.9. the head of an international intergovernmental organization, his deputy, a member of the management or supervisory body;

5.12.3.10. the head of a political party, his deputy, a member of the governing body of the political party.

5.12.4. Immediate family members are: spouse/partner, parents, brothers, sisters, children and children's spouses/partners.

5.12.5. Close associate is:

5.12.5.1. a natural person who holds ownership in the same legal person or an organization without legal personality or maintains other business relations with a PEP;

5.12.5.2. a natural person who is the sole beneficiary of a legal person or an organization without legal personality, established or operating for the de facto property or other personal benefit of a PEP.

5.12.6. The status of PEP shall remain for 12 (twelve) months following resignation from the respective position indicated in Art. 5.11.3 of the Policy.

5.12.7. In order to establish whether the Client (in case of Client legal person - the beneficiary, director(-s) and representative(-s) of the Client) is a PEP, the Company shall request the Client to provide such information by the Client himself/herself/itself and shall verify it against official databases. The Company will

use automated solution to verify of the Client is a PEP. Such verification shall be continuous.

5.12.8. In case during the onboarding of the Client the Company shall establish that the Client is a PEP, such Client will be subject to EDD.

5.13. Ongoing due diligence (ODD)

5.13.1. The ongoing due diligence obligation comprises two aspects:

5.13.1.1. on the one hand, the obligation to carefully examine the transactions carried out over the course of the business relationship with the Clients; this obligation includes monitoring the Client's occasional transactions and paying attention to intriguing facts related to the Client which, if they are suspect, should be duly investigated and, if necessary, reported to FIU; and

5.13.1.2. on the other hand, the obligation to update the data or information collected as part of the identification and identity verification obligation and the obligation to identify the Client's characteristics and the purpose and nature of the business relationship or the occasional transaction.

5.13.2. In implementing the ODD, the Company shall adopt a risk-based approach: the level of ODD to be exercised by the Company must be proportionate to the level of risk identified in the Client's individual risk assessment (as defined in *Customer Risk Assessment procedure* of the Company), taking into account, where appropriate, any updates of this assessment. I.e. the more thorough and detailed ODD shall be performed in relation to the higher risk Clients.

5.13.3. Regarding monitoring, both in real time and retrospective, of the Clients' transactions in order to identify activity that is inconsistent with the Company's knowledge of the Client and business relationship refer to Art. 5.1.3 of the Policy.

5.13.4. Regarding reviewing Client identification records and keeping information about the Client up to date refer to Art. 5.14 of the Policy.

5.13.5. The ODD also includes continuous screening of the Company's Clients against international financial sanctions and international restrictive measures and PEPs lists. While screening the Clients legal person, its beneficiaries, directors and representatives must be screened as well. In case during such screening it is established that the Client has been included in the list of international financial sanctions and international restrictive measures procedure indicated in the Company's Procedure regarding Implementation of international financial sanctions and restrictive measures shall be invoked.

5.14. Transaction monitoring

5.14.1. Objectives of monitoring are the following:

5.14.1.1. To identify suspicious transactions;

5.14.1.2. To ensure the relevance of the Client and beneficiary data, the purpose and nature of the business relationship;

5.14.1.3. To ensure the relevance of the Client's risk in the event of a change in circumstances;

5.14.1.4. To determine whether the Client's transactions correspond to the information previously collected on the Client;

5.14.1.5. To properly understand the Client's activities and to create exhaustive Client's file; and

5.14.1.6. To make sure that the transactions are not related to illicit activity;

5.14.1.7. To follow IP addresses of the Clients;

5.14.1.8. To notice changes in sanctions and relevant lists for the names of the Clients, both natural and legal,

5.14.1.9. To identify newly provided websites, newly added payout/withdrawal settings, i.e. bank accounts and any other payment accounts; and

5.14.1.10. To notice dormant accounts reactivated.

5.14.2. The Company must conduct continuous monitoring of the Client's transactions in order to ensure that the executed transactions correspond to the Company's knowledge on the Client, Client's business (type of business and its nature, nature of transactions, business partners, area of activity, etc.), nature of risk and knowledge about the source of funds.

5.14.3. Information must be collected in such a way that the purpose and nature of the transactions executed could be clearly understood. Information collected on the Client should include information including, but not limited to: from where funds are transferred to the Client's account, where the funds are transferred by the Client, how often transactions are performed, in what currency transactions are performed, what transactions the Client performs most often etc which would help to create the Client's portrait.

5.14.4. When conducting the transaction monitoring, the Company will focus particular emphasis on the following:

5.14.4.1. Transactions that, by virtue of their nature, may be related to ML/TF, and complicated and unusually large transactions in particular, as well as any unusual transactions structures that do not have an evident economic or visible legal goal. The Company shall investigate the grounds and purpose of such transactions and shall document the results of the investigation in writing;

5.14.4.2. Every ML/TF threat that may arise due to usage of products of any nature, other results of human labour, usage of the services provided, or transactions being carried out, when efforts are made to conceal the identity of the Client or the beneficiary (leaning towards anonymity), as well as due to business relationship with the Client who was not identified being present in person, and, where applicable, shall immediately take measures in order to prevent the funds being used for ML/TF purposes;

5.14.4.3. whether the Client has no connections with countries that fall within the higher-risk category countries: which are subject to European Union sanctions or other restrictions, as well as with countries that are classed by the FATF as high-risk or non-cooperative countries, and so on;

5.14.4.4. the duty to immediately take measures in order to prevent ML/TF.

5.14.5. The monitoring of the business relationship shall be exercised on a regular basis, keeping information on measures applied in the process of monitoring and information collected in the process of taking such actions, keeping information on the purpose and nature of business relationship, and making reviews and updates of such information on a regular basis. Business relationship of the Clients assigned with a higher risk will be reviewed more frequently than of other Clients.

5.14.6. If the monitoring of business relationship indicates that the business relationship entails a higher risk, then the Company shall assign such Client to the higher risk group.

5.14.7. Information obtained in the process of analysing the Client's activity shall be continuously documented and shall be kept in written or electronic form.

5.14.8. The Clients that are subject to transaction monitoring may:

5.14.8.1. be required to provide additional KYC information;

5.14.8.2. be subject to EDD;

5.14.8.3. be subject to termination of the business relationship.

5.14.8.4. Nothing, it may be that the outcome of monitoring reveals an acceptable explanation for the initially suspicious transaction or operation

5.14.9. The following additional actions may be performed during the enhanced monitoring: (a) additional review of the Client's transactions according to a schedule approved by the Money Laundering Reporting; or/and (b) setting tailored transaction thresholds that, when exceeded, would immediately trigger business relationship monitoring and analysis actions; and/or (c) each transaction of the Client is being processed only after checking that it does not hit any of the criteria to be considered as suspicious.

5.14.10. Transaction monitoring is detailed in the Transaction monitoring procedure.

5.15. Periodic reviews

5.15.1. The Company must keep up to date the data or information the Company holds pursuant to its obligation to identify and verify the identity and its obligation to identify the characteristics of the Client, as well as the purpose and nature of the business relationship or the transaction.

■ This updating obligation is an important prerequisite for detecting atypical transactions: if the Company cannot rely on current information, the ongoing due diligence measures with respect to the transactions monitoring may not allow to identify the atypical character of some of them or, conversely, transactions could unnecessarily be treated as atypical whereas they would have been considered as not requiring special attention if the information held by the Company had been updated.

5.15.2. This updating obligation applies as soon as the relevant elements that are taken into account in the context of the individual risk assessment are modified. In complying with this obligation, a risk-based approach should be adopted. Thus, the

measures taken by the Company to fulfil this obligation should be proportional to the risk identified in the context of the individual risk assessment. However, it should be noted that the updating of data and information is of particular importance where elements relevant to the individual risk assessment appear to be no longer current. The Company must also take into account this potentially higher level of ML/FT risk presented by a given situation in determining the updating measures to be taken.

5.15.3. Taking into account Art. 5.14.2 of the Policy, periodic reviews shall be performed in the following periodicity:

5.15.3.1. For high risk Clients - every 12 (twelve) months;

5.15.3.2. For medium risk Clients - every 2 (two) years.

5.15.3.3. For low risk Clients - every 3 (three) years.

- The Company may establish individual periodicity regarding specific Clients shall the Company sees that as necessary. Such individual periodic review cannot be less common than initially establish for the risk level to which the Client is assigned.
- Also, it must be noted, however, that if the Company knows or cannot be unaware that data relevant for the individual risk assessment is modified the Company must perform review of the Client irrespective if the term relevant to a certain Client has not yet elapsed.

5.15.4. Periodic review must cover all the data collected in the context of the initial identification, and not only separate parts of such data. Similarly, the verification of the updated data may not be less comprehensive than that of the initial identification data.

5.15.5. The Company's obligation to update the information the Company holds about its Clients includes the obligation to implement measures to identify the persons among the Company's Clients whose individual situation has changed to such an extent that such persons fall within enhanced due diligence measures are required by the Law.

5.15.6. All changes and updates in the Client's information must be properly documented to ensure the existence of audit trail.

5.15.7. Periodic review is detailed in the Company's Periodic review procedure.

5.16. Need to re-verify Clients

5.16.1. If at any time, the Company has reasonable grounds to doubt whether an existing Client is the person they claim to be, the Company must within 14 calendar days of formation of that opinion, take appropriate and reasonable steps to make sure as to the true identity of the Client including undertaking Client KYC procedures.

5.17. Client file

5.17.1. Information obtained in the process of identifying the Client and the beneficiary hall be continuously documented and shall be kept in electronic form.

5.17.2. The Client file shall consist, as a minimum, of the following documents:

5.17.2.1. the documents and information collected in the process of the Client and the beneficiary identification;

5.17.2.2. proof of verification of the identity of the Client, the Client's representative (if applicable), and the UBO in reliable and independent sources of data;

5.17.2.3. proof of verification of the political exposure of the Client, the Client's representative (if applicable), and the beneficiary in public and independent sources of data;

5.17.2.4. a description of the Client's risk profile;

5.17.2.5. a description of the Client's assignment to a risk group;

5.17.2.6. information about the services and products provided to the Client;

5.17.2.7. information about cases when the Client made suspicious transactions (if any) and the outcome of the investigation of such suspicious transactions; and

5.17.2.8. Recommendation for or against on-boarding.

5.18. Abandoned and dormant accounts

5.18.1. Such accounts that become active again shall be closely monitored for additional suspicious activity.

5.19. Prohibited Clients

5.19.1. The Company shall not establish business relationship in the following cases:

5.19.1.1. when the Company is unable to the meet the requirements of the Law (e.g. cannot conduct proper monitoring of the business relationship with the Client);

5.19.1.2. where the Client fails to provide identification all data or such data is incorrect or insufficient or the Client or its representative avoids or fails (i.e. provided data is not sufficient) to provide the information necessary to identify the beneficiary, conceals the identity of the beneficiary or fails to provide the information necessary to identify the beneficiary;

5.19.1.3. where the Company cannot establish if the Client is acting of his/her/its own and identify the beneficiary and the representative, if the Client is acting through representative;

5.19.1.4. where the Company cannot establish and understand the organizational and management structure of the Client legal person;

5.19.1.5. where the Company cannot establish and understand the Client legal person activities;

5.19.1.6. where the Company cannot establish and understand the nature of the business relationship with the Client;

5.19.1.7. where the Company cannot establish and understand the purpose of the business relationship with the Client;

5.19.1.8. where the Company cannot verify identity of the Client or the beneficiary against data/documents/information obtained from independent and reliable source;

5.19.1.9. where the Company cannot perform ongoing due diligence of the business relationship with the Client.

- In the cases indicated above the Company having assessed the threat of ML/TF, shall decide on the

expediency of filling suspicious activity report to FIU.

5.19.2. In addition to the above, the Company shall not establish business relationship in the following cases:

5.19.2.1. The Client's activities are included in the Company's list of prohibited activities;

5.19.2.2. The Client is a citizen of or resides in or the Client legal person is established or operates in prohibited jurisdiction;

5.19.2.3. International financial sanctions or other restrictive measures are applicable against the Client;

5.19.2.4. The Client has or had connections/links with organized criminal organizations;

5.19.2.5. The Client is or was associated in the past with sources of revenue received from organized crime (e.g. smuggling of drugs or excise goods, illegal trade in arms or human organs; trade in prostitution services; the management of brothels; international money transfers without the appropriate permits (such as E-gold); underground banking (such as Hawala); lotteries, betting or casino operation without permits from competent public authorities etc);

5.19.2.6. The ML/TF risk posed by the Client exceeds the Company's risk appetite.

5.19.3. The Company will not open anonymous accounts or accounts under obviously fictitious names, as well as shall not enter into the business relationships without requesting and obtaining the Client's and beneficiary identification data or if there is a reasonable suspicion that these documents contain fraudulent data or are counterfeit.

5.19.4. If, during the establishment of the identity of the Client, suspicion that ML/TF is being conducted arises, and the further process of establishing the identity of the Client and the beneficiary may give rise to the suspicions that the Client may be

disclosed to the competent law enforcement authorities, the Company may discontinue the establishment of the identity of the Client and the beneficiary and shall not enter into a business relationship with the such Client. In such case, suspicious activity report shall be filled to the FIU (refer to Art. 6.2 of the Policy).

6. Complex or unusually large transactions and unusual transaction structures

6.1.1. The Company must draw its attention such Clients' activities which, in its opinion, may, by their nature, involve ML/TF, and in particular:

6.1.1.1. Complex transactions;

6.1.1.2. Unusually large transactions;

6.1.1.3. Transactions that are executed in unusual way;

6.1.1.4. Structure of any unusual transaction that do not have a clear economic or visible legitimate purpose;

6.1.1.5. business relationships or transactions with Clients from third countries where, according to information officially published by international intergovernmental organizations, measures to prevent ML/TF are insufficient or do not comply with international standards.

6.1.2. In case the Company established any of the above in respect of its Client, the Company must investigate the basis and purpose of the transactions and record the results of the investigation in writing. After assessing the threat of possible ML/TF, the Company shall decide on the expediency of filing a SAR to the FIU (FNTT). Further on, enhanced ODD of business relationships with such Client should be applicable.

7. Suspicious transactions

7.1. General

7.1.1. Suspicious transactions are identified by the Company taking into account such Clients' activities that, in the Company's opinion, may be related to ML/TF (a) during verification of the identity of the Client and the beneficiary; (b) while performing continuous ODD of the business relationship with the Client, including investigation of the transactions that have executed during the term of the business relationship; and (c) taking into consideration the criteria for identifying suspicious transactions approved by the FIU (FNTT). Follow this link to the criteria for identifying suspicious transactions approved by the FIU: Criteria. The Company may establish additional criteria (on top of those approved by FIU) for identifying suspicious transactions considering peculiarities of its business, its Clients, products, services and jurisdictions.

7.1.2. If the transaction does not meet any of the criteria either listed in the FIU list or indicated by the Company, however, the Company's employee has a suspicion regarding the transaction and/or the Client's activities, such Transaction shall also

be considered as suspicious transaction and shall be subject to further actions set forth in Art. 7.2 Suspicion may be caused by various objective and subjective circumstances, e.g., the Client executes transaction(-s) that is not typical for the Client's activities, provides incorrect data about himself/herself/itself or the transaction at hand, avoids providing additional information/data/documents requested by the Company.

7.1.3. If the Company (employees) identifies the transaction as suspicious, the Company must perform internal investigation to either confirm or deny its suspicions. The Company must understand the purpose and the logic and economic reasoning of the transaction, source of funds used to execute such transaction etc.

7.1.4. An internal investigation must be based on (a) on data/documents/information either already collected/held by the Company or newly requested to be provided to the Company by the Client (depending on the case); (b) overall Company's knowledge on the Client (i.e. suspicious transaction cannot be investigated separately, without taking into consideration any and all data/documents/information obtained on the Client, adverse media findings, outcomes of other internal investigations (if any), transactions history in Client's payment account; (c) general understanding of the Client's business activities (i.e. taking into consideration the characteristic of certain industry) and the ML/TF risks that such activities raise. Internal investigation must be made in writing and documented in detail, in a manner that any third party may be able to make use of such description (i.e. new employee or representative of the supervisory body or law enforcement body be able to understand the investigation, its reason, outcome and the arguments the outcome was made on). The same principles of investigation are applicable when analysing complex or unusually large transactions and unusual transaction structures. Performance of internal investigation is detailed in the Company's Internal investigation procedure.

7.1.5. The Company shall have no obligation to establish whether the Client's act contains a criminal offense. The Company must notify the FIU (FNTT) if it knows or suspects that a transaction is suspicious. However, the Company must ensure that none of its employees would tip-off the Client or would inform any other third party that the information has been submitted to the FIU. The Company must ensure that its employees are well aware and trained how to act in such situations.

7.2. Filing of suspicious activities reports (SARs)

7.2.1. If it has been determined that the Client is executing a suspicious transaction, the Company must suspend that transaction and file SAR to FIU (FNTT) no later than within 3 (three) business hours following the suspension of the suspicious transaction. Obligation to report is not subject to the amount of the suspicious transactions.

■ For the purpose of this clause, determination is the outcome of internal investigation (please refer to Arts. 7.1.3-7.1.4).

7.2.2. The Company may not suspend the suspicious transaction if due to the nature of the transaction, the manner of its performance or other circumstances it is not objectively possible to do so. In such a case, the SAR must be filed to FIU (FNTT)

within 3 (three) business hours following the determination of the suspicious transaction.

7.2.3. The Company must immediately inform the FIU (FNTT) upon receipt of information that the Client intends to or will attempt to perform a suspicious transaction. Upon submission of such notification and receipt of the approval of the FIU (FNTT), the Company may not perform the actions necessary for the execution of the intended transaction. If such actions are being performed, the suspicious transaction must be suspended. Notification is submitted in a form of SAR.

7.2.4. Filing of SAR is detailed in the company's Procedure regarding reporting to authorities.

7.2.5. In addition to filing SARs as indicated above, the Company must immediately, not later than within 1 (one) business day following the receipt of respective knowledge or the occurrence suspicion, notify the FIU (FNTT) if the Company is aware or suspects that the assets of any value is obtained directly or indirectly from or participating in a criminal offense, and the Company is aware or suspects that such assets is intended to support one or several terrorists or a terrorist organization.

7.2.6. The Company shall not be liable to its Clients for non-performance of contractual obligations and damage caused by the performance of the Company's obligations to report to the FIU (FNTT) or obligatory instructions issued by the FIU (FNTT) to the Company. The Company's Management and other employees who in good faith filed SAR regarding suspected ML/TF or suspicious transaction(-s) carried out by the Client to their leader or the FIU (FNTT) shall also not be held legally liable and they may not be subject to disciplinary action in relation thereof.

7.3. Actions by the FIU (FNTT) following the submission of SAR

7.3.1. Upon receipt of SAR, the FIU (FNTT) shall perform the actions necessary to substantiate or deny doubts regarding the executed or being performed criminal act by the Client within 10 (ten) business following the receipt SAR.

7.3.2. If during of investigation of the SAR, the FIU (FNTT) requests the Company to provide any additional information/data/documents in relation thereto, the Company must submit the requested information/data/documents within 1 (one) business day following the receipt of the request in requested form and manner.

7.3.3. Once the legitimacy of the funds or assets is substantiated or doubts regarding possible links with the TF are denied, the FIU (FNTT) shall immediately notify the Company in writing that the transaction(-s) may be resumed.

7.3.4. If the Company is not obliged to apply the temporary restriction of ownership rights in accordance with the procedure established by the Code of Criminal Procedure of the Republic of Lithuania, the transaction must be renewed.

7.3.5. If suspension of the transaction may interfere with the investigation of ML or assets legalization (acquired in a criminal way), TF and other criminal acts related to ML/TF, the FIU (FNTT) shall notify the Company thereof. Upon receipt of a written notice from the FIU (FNTT) that the suspension of the transaction may interfere with the investigation of ML or assets legalization (acquired in a criminal way), TF and other criminal acts related to ML/TF, the Company shall not suspend the Client's

suspicious transactions and shall immediately resume suspended suspicious transactions.

7.4. Instructions issued by the FIU (FNTT) to suspend suspicious transaction(-s)

7.4.1. Upon receipt of written instructions by the FIU (FNTT) regarding suspension of suspicious transaction(-s) performed by the Client, the Company must suspend this transaction(-s) for up to 10 (ten) Business days from the time specified therein or the occurrence of specific circumstances.

7.4.2. Upon issuance of written instructions to suspend suspicious transaction(-s), the FIU (FNTT) shall perform the actions necessary to substantiate or deny doubts regarding the executed or being performed criminal act by the Client within 10 (ten) business following the receipt SAR.

7.4.3. If during of investigation of the suspicious transaction(-s) (instructions regarding which was issued), the FIU (FNTT) requests the Company to provide any additional information/data/documents in relation thereto, the Company must submit the requested information/data/documents within 1 (one) Business day following the receipt of the request in requested form and manner.

7.4.4. Once the legitimacy of the funds or assets is substantiated or doubts regarding possible links with the TF are denied, the FIU (FNTT) shall immediately notify the Company in writing that the transaction(-s) may be resumed.

7.4.5. If the Company is not obliged to apply the temporary restriction of ownership rights in accordance with the procedure established by the Code of Criminal Procedure of the Republic of Lithuania, the transaction must be renewed.

7.4.6. If suspension of the transaction may interfere with the investigation of ML or assets legalization (acquired in a criminal way), TF and other criminal acts related to ML/TF, the FIU (FNTT) shall notify the Company thereof. Upon receipt of a written notice from the FIU (FNTT) that the suspension of the transaction may interfere with the investigation of ML or assets legalization (acquired in a criminal way), TF and other criminal acts related to ML/TF, the Company shall not suspend the Client's suspicious transactions and shall immediately resume suspended suspicious transactions.

7.5. Protection of information submitted to the FIU (FNTT)

7.5.1. The Company and its employees are prohibited from notifying the Client or other persons that information about the Client's transactions that are being performed or have been executed or any other information has been submitted to the FIU (FNTT) or another supervisory authority.

7.5.2. The information that has been submitted to the FIU (FNTT) in accordance with this Policy, may not be published or transferred to other state management, control or law enforcement institutions, other persons, except for the cases specified in the Law and other laws.

7.5.3. Unless otherwise specified by the FIU (FNTT), the prohibition set forth in Art. 7.5.1 of this Policy does not prohibit the exchange of information between financial institutions, auditors, accounting or tax consulting companies, notaries, notary

representatives and persons entitled to perform notarial acts and lawyers and assistant lawyers in cases that are related to the same Client and the same transaction involving two or more of the entities referred to in this clause, if such entities are registered in the EU member states or in a third country where requirements equivalent to those established by the Law apply to them and if they belong to the same category and have equivalent obligations of professional secrecy and protection of personal data. The foregoing exchange of information is permitted only for the purpose of preventing ML/TF.

■ However, exception is clause shall may not be valid if a separate decision of the European Commission has been adopted in this regard.

7.5.4. In the cases indicated in Art. 7.5.3 of the Policy, if personal data is provided during exchange of information with entities registered in third countries, the provision of personal data must comply with the requirements of Paragraph V of the Regulations (EU) 2016/679.

7.5.5. The Law on Legal Protection of Personal Data of the Republic of Lithuania.

7.5.6. Persons who have violated the procedure for storage and use of information specified in the Law and this Policy shall be held liable in accordance with applicable law.

7.5.7. Submission of the information indicated in the Policy to the FIU (FNTT) shall not be considered as disclosure of industrial, commercial or banking secrets or other confidential information.

8. Implementation of international financial sanctions and restrictive measures

8.1. The Company must enforce international financial sanctions and restrictive measures and perform the actions set forth in the Instructions for supervision of proper implementation of international financial sanctions by the FIU (FNTT) under the Ministry of Interior of the Republic of Lithuania and EU Regulations on international sanctions and their exemptions.

8.2. It must be verified if the Company's Clients, their representatives and beneficiaries are not included in the lists of persons subject to international financial sanctions and restrictive measures.

8.3. Verification indicated in Art. 8.2 of the Policy is performed during establishment of the Client's identity, as well as by conducting the ODD of the Client's business relationships, executing the Client's transactions.

8.4. Implementation of international financial sanctions and restrictive measures is detailed in the Company's Procedure regarding Implementation of international financial sanctions and restrictive measures.

9. Termination of transactions or business relationship

9.1. The Company may refuse to execute the Client's transaction(-s), terminate the transaction(-s) or terminate business relationships with the Client in the following cases:

9.1.1. If the Client avoids or refuses to provide the Company with additional information at its request and within the term set by the Company and therefore, the Company cannot effectively manage ML/TF risk posed by the Client;

9.1.2. While performing ODD, the Company identifies the change of ML/TF risk in such scope that the Company is not able to effectively mitigate such risk and cannot properly perform obligations implied on the Company by the Law;

9.1.3. The Company is unable to meet the following requirements: the Client fails to provide data confirming his/her/it identity in the cases specified in the Policy, the Client or its representative avoids providing information necessary to identify the beneficiary, hides the identity of the beneficiary or avoids providing information necessary to identify the beneficiary, or the data provided is insufficient; the Company is unable to ensure the fulfilment of the requirements to establish whether the Client acts on its own behalf or is under control; to identify the beneficiary and the representative of the Client; to understand the activities of the Client, ownership and organizational structure of the Client legal person.

■ The Company must assess the threat posed by the ML/TF in the above cases and decide on the expediency of filing SAR with FIU (FNTT).

9.2. Refusal to execute the Client's transaction(-s), termination of the transaction(-s) or termination business relationships with the Client must be well documented in writing indicating the reasons of the outcome.

9.3. The Company shall not be held liable against the Client for non-performance of contractual obligations and damage caused due to non-performance of the Client's transaction(-s), if the Client's transaction(-) was not performed due to reasons indicated in Art. 9.1 of the Policy.

10. Information storage

10.1. Registration logs

10.1.1. The Company maintains the following logs:

10.1.1.1. Log of suspicious transactions;

10.1.1.2. Log of SARs filed to the FIU (FNTT) in accordance with this Policy;

10.1.1.3. Log of one-off or several related transactions amount of which is equal or exceeds €15,000 or equivalent amount in foreign currency;

10.1.1.4. Log of transactions received and sent in accordance with Regulation (EU) 2015/847 of the European Parliament and of the Council on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 as of 20 May 2015; and

10.1.1.5. Log of Clients' business relationship with which have been terminated in accordance with Art. 9.1.1 of the Policy or due to other violations of prevention of ML/TF.

10.1.2. Processing of the registration logs is detailed in the Company's Procedure on Registration log.

10.2. Retention of beneficiary data

10.2.1. The Company must collect and, upon the request of the FIU (FNTT), provide the following data on the beneficiary:

10.2.1.1. Beneficiary's identification data;

10.2.1.2. Evidence of verification of the information provided by the Client in reliable and independent sources;

10.2.1.3. Data on the Client's legal person ownership and management structure.

10.3. Form and period of information storage

10.3.1. All data/documents/information shall be stored in electronic medium.

10.3.2. The data of the registration logs indicated in Art. 9.1.1 of the Policy shall be stored for 8 (eight) years following the date of termination of transactions or business relations with the Client.

10.3.3. Copies of the Client's identification documents, beneficiary's identity data, beneficiary's identity data, recording of live video transmission (live video broadcast), other data obtained during the Client's identification, invoices and/or agreements must be kept for 8 (eight) years following the date of termination of transactions or business relationship with the Client.

10.3.4. Correspondence with the Client in relation to the business relationship of the must be kept for 5 (five) years following the date of termination of the transactions or business relationship with the Client.

10.3.5. Documents and data confirming the transaction, or other legally valid documents and data related to the execution of the transactions must be kept for 8 years from the date of execution the transaction.

10.3.6. Outcome of investigations indicated in Art. 7.2.1 of the Policy must be kept for 5 (years) years.

10.3.7. Retention period of the data indicated in the paragraph may be extended for a further period not exceeding 2 (two) years upon reasoned instruction from the competent authority.

10.3.8. The Company must ensure that:

10.3.8.1. The documents and information in this Paragraph shall be stored regardless of whether:

a) Transactions are domestic or international;

b) The business relationship with the Client continues or has ended;

10.3.8.2. The documents and information in this Paragraph shall be stored in such a way that it is possible to:

a) Restore specific transactions;

b) Upon request submit such transactions and the information contained therein to the FIU (FNTT) or to other competent authorities.

11.Training

11.1. The Company must take appropriate measures to ensure that its employees are aware of the requirements of the Law. To ensure this Company maintains comprehensive *Corporate training policy* and *AML-CTF-Sanctions training procedure*. Such measures shall include the participation of relevant staff in internal and external general training regarding prevention of ML/TF and specific continuing training programs to train to identify actions that may be related to ML/TF and how to deal with them.

11.2. The Company must ensure that new employees whose functions shall require application of the Policy are first familiarized with the Policy (at least to the extent necessary for the proper performance of the functions of a particular employee). For the foregoing purpose the Company must prepare respective training/familiarization tools/instructions.

11.3. According to the functions of the respective employees, the Company must prepare a list of positions that must be familiarized with the Policy.

11.4. The training is carried out through internal training and external training, as well as using publicly available relevant courses and materials.

11.5. To ensure that training material is up to date, it must be reviewed and updated periodically. The relevant Company's staff must be informed of such updates in a manner (via email, additional live training session) that best suits the scope of update.

11.6. To ensure that the knowledge of the Company's employees is up to date, employees must be regularly informed about existing and new requirements on prevention of ML/TF (at least one year after the last training). The Company must assess the ability of each employee to hold office taking into consideration the requirements on prevention of ML/TF in respect of relevant position.

11.7. Training material must include at least the following:

11.7.1. introduction to the concept of ML/TF to ensure that all employees understand what ML/TF is, how to recognize ML/TF and the importance of prevention of ML/TF;

11.7.2. requirements of Client's identification (including application of EDD measures), filing of SARs (including, but not limited to informing employees that they may not disclose filing of SAR and its content to any third party (including the Client) and informing the employees that they shall not have any negative consequences due to the notification of possible ML/TF case to the FIU (FNTT) or the Company's management;

11.7.3. maintenance of registration logs and sanctions for non-compliance with the foregoing requirements;

11.7.4. requirements and importance of ODD;

11.7.5. training intended to teach the staff to identify possible ML/TF cases;

11.7.6. implementation of international financial sanctions and restrictive measures; and

11.7.7. familiarization of employees with their specific responsibilities applying the Policy.

11.8. If there is a need, the following training may be conducted in the Company:

11.8.1. Tailored training intended to target the specific area of prevention of ML/TF. Such tailored trainings shall be intended for all or part of the employees whose duties include handling of the Clients' business;

11.8.2. Tailored training intended for senior management;

11.8.3. Tailored training intended to analyse ML/TF related incidents;

11.8.4. Tailored training regarding adoption of new technologies to be used for the prevention of ML/TF;

11.8.5. Tailored training regarding changes in the applicable law.

11.9. The Company stores information on all training performed for the purpose of prevention of ML/TF, including the date of such training, materials, employees who participated in the training, as well as tests (if applicable). Participation in training shall be verified by the signature of the employee who took part in the training.

12.Internal control

12.1. Internal control shall ensure that the Company (including all its employees and outsourced services providers) shall comply with requirements regarding prevention of ML/TF set forth in the Law and other legal acts related to prevention of ML/TF. The Company's Money Laundering Reporting Officer shall be responsible to ensure implementation of internal control indicated in this Paragraph.

12.2. Internal control is based on vertical and horizontal three lines of defence:

12.2.1. Horizontal three lines of defence: (a) risk management; (b) compliance; and (b) internal audit;

12.2.2. Vertical three lines of defence: (a) sales person is accountable to the manager; (b) MLRO is accountable to the Managing Director (CEO) and the Management Board; and (c) the internal auditor shall only report to the Company's Management Board.

12.3. The Money Laundering Reporting Officer shall ensure daily compliance with the Law and other legal acts related to prevention of ML/TF and shall apply the following measures:

12.3.1. continuously investigates the Company's Client identification process, i.e. reviews whether all mandatory actions have been taken consistently and methodically while identifying the Clients, the necessary information has been collected, the necessary documents have been obtained, the information has been properly verified etc. The Money Laundering Reporting Officer shall be entitled to perform such investigation at any time, to the chosen, extent and other employees of the Company or outsourced services providers must cooperate with the Money Laundering Reporting Officer .

■ All identified deficiencies shall be recorded in writing by the Money Laundering Reporting Officer, as well indicating the reasons for the identified deficiencies. The member of the Management Board assigned to ensure implementation of the Law, shall be informed on the identified deficiencies and shall be obliged to take corrective actions immediately. The Money Laundering Reporting Officer shall be notified once identified deficiencies have been cured;

12.3.2. pays detailed attention to the Clients who are subject to EDD and respectively enhanced ODD;

12.3.3. assesses whether the Company uses up to date information while assessing its Clients' risk (e.g. information regarding risks posed by the Company's products, geographical risks, up to date lists of international financial sanctions and restrictive measures etc.);

12.3.4. assesses application of ODD and respectively enhanced ODD, including but not limited to monitoring of Clients' transactions;

12.3.5. assesses whether the Clients and the beneficiaries' identity data is updated in proper and timely manner in accordance with the Policy and the Law;

12.3.6. reviews SARs filed to the FIU (FNTT), assesses whether all SARs were files in accordance with the applicable law and established internal procedures, deadlines, indicating all necessary information, assesses whether submission of SARs was reasonable in all cases and on the contrary, whether there were cases where SAR had to be filed (however, was not) and respectively establishes the reasons thereof;

12.3.7. reviews the registration logs kept by the Company, assesses whether the registration logs are filled in properly, they contain all the mandatory information according to which a specific transaction may be identified. The Compliance Officer having identified deficiencies in filling in the registration logs, shall establish the reasons thereof and propose measures to eliminate identified discrepancies;

12.3.8. assesses exchange of information within the Company regarding implementation of procedures and measures of prevention of ML/TF, i.e. whether such information is made available to other Company's employees in a timely manner and to the required extent etc;

12.3.9. ensures proper and timely training to the Company's employees. The Compliance Officer shall ensure that practical cases in relation to established deficiencies of implementation of prevention of ML/TF are analysed during training, including the reasons thereof and measures required/implemented to avoid such cases in the future.

12.4. In addition to above, the Compliance Officer shall fill in a detailed report regarding implementation of prevention of ML/TF in the Company at least twice a year.

12.5. Results of internal control (together with the proposal how to cure the identified shortcomings) shall be indicated in writing and provided to the Company's Managing Director (CEO), the Management Board, Risk Manager and according to the specific needs to the Company's business units managers and/or employees. The Company must ensure that the identified shortcomings are cures in proper and timely manner.

12.6. The Money Laundering Reporting Officer shall submit proposals regarding elimination of identified deficiencies in prevention of ML/TF and subsequently check how such deficiencies have been eliminated.

12.7. Internal control regarding processing of personal data for the purpose of prevention of ML/TF shall be performed by the Company's Data Protection Officer.

12.8. Money Laundering Reporting Officer shall be responsible for proper management of business-wide ML/TF risks.

13.Review of the Policy

13.1. The Policy is reviewed at least once per year or immediately after relevant applicable law changes or other significant circumstances occur. Where necessary, the relevant amendments are to be made.

13.2. The review must assess:

13.2.1. the effectiveness of the Policy, having regard to the ML/TF risk;

13.2.2. whether the Policy complies with the regulatory requirements;

13.2.3. whether the Company has effectively implemented the Policy; and

13.2.4. whether the Company has complied with the Policy.

13.3. The Money Laundering Reporting: must:

13.3.1. Ensure the amendment of the Policy taking into account of any deficiencies identified in the review;

13.3.2. Develop a plan (with appropriate training) for implementation of the amendments of the Policy; and

13.3.3. Manage the conduct of the developed plan.

13.4. The Money Laundering Reporting Officer must keep a breach register which contains details of any breaches or failure to comply with the Policy. On an annual basis, the Money Laundering Reporting Officer must review the breaches register and consider whether the breaches or non-compliance which occurred during the relevant period indicate any systemic deficiencies in the Policy and recommend to the Company's management how these deficiencies ought to be rectified.

13.5. The process of blacklisting data on the Company's system is to protect the Company from illicit and fraudulent use. Data points that might be added to the blacklist include but are not limited to email addresses, IP addresses, websites, as well as legal and natural person's names. Such data points are used to compare against information being added to or found on the Company's system and matches or potential matches may stop the activity and/or trigger an alert for the Company's Money Laundering Reporting Officer to review.

13.6. Data points are added to the blacklist on a regular basis. Data points are added from internal investigations or external reports which are made known to the Company or if the Company discovers by other means, e.g. news articles, subpoenas, laws, official lists maintained by other governmental institutions.

13.7. Data points found by any other employee of the Company must be shared with the Money Laundering Reporting Officer their findings, where the data point(s) was/were found and why they believe the data point(s) is/are relevant for blacklisting.

14.Final provisions

14.1. The Policy shall be treated as confidential internal document and, therefore, shall not be distributed outside the Company.

14.2. Employees are informed in writing of the approval and amendment of the Policy or other documentation in relation of the Policy. The member of the Company's Management Board who has been appointed as a responsible person to ensure proper implementation of prevention of ML/TF shall be responsible for communicating relevant changes.

14.3. New employees in compliance/AML/onboarding and risk departments/positions shall be familiarized with the Policy on their first working day in writing. Other employees shall be introduced to the concept of AML/CTF whereas compliance with the requirements regarding prevention of ML/TF is of the critical importance for the successful operation of the Company.

15. Summary of changes

Version	Revision date	Revised by:	Summary of changes:
1.0	2021-02-25	External legal counsel	Initial version
2.0	2023-09-18	MLRO	Changes in various sections of the document in relation to Client risk assessment and AML/CTF trainings. Added second remote identification method. Included SDD (simplified due diligence).

Annex 1. Money laundering (ML) and Terrorist Financing (TF)

1. Money Laundering (ML)

1.1. Money laundering shall mean: the process of taking illegally obtained and/or illegitimate funds and hiding their source. The source of illegally obtained or illegitimate funds may come from theft, counterfeiting and/or any other criminal activity. The ultimate goal from laundered funds is to make it seem like those funds are in fact legitimate and/or derived by legal means.

1.2. When a criminal activity generates substantial profits, the individual or group involved must find a way to use the funds without drawing attention to the underlying activity or persons involved in generating such profits. Criminals achieve this goal by disguising the source of funds, changing the form or moving the money to a place where it is less likely to attract attention. Criminal activities that lead to ML (i.e., predicate crimes) can include: illegal arms sales, narcotics trafficking, contraband smuggling and other activities related to organized crime, embezzlement, insider trading, bribery and computer fraud schemes. ML can be achieved through virtually every medium, financial institution or business.

1.3. The laundering process is often described as taking place in three stages as elaborated below. The three basic stages may occur as separate and distinct phases. They may also occur simultaneously or, more commonly, may overlap.

Stage	Description
Placement	The first stage of ML and also the stage with the highest risk of getting caught. This stage is where the criminals put their assets into the financial system. Examples of placement include: ● mixing of legitimate funds with illegitimate funds, such as combing the cash from illegal narcotics sales with that of a cash-intensive locally owned restaurant, salon or kebab shop;1 ● foreign exchange: purchasing of foreign currency with the illegal funds; ● structuring or smurfing: depositing various smaller amounts into numerous bank accounts in an attempt to evade reporting thresholds, most common thresholds being 10k EUR/USD; ● currency smuggling: cross-border physical movement of cash or monetary instruments to deposit into foreign bank accounts; ● asset conversion: it simply involves the purchase of goods. Illegal money is converted into other assets, such as real estate, diamonds, gold and vehicles, which can then be sold, and proceeds can be deposited in the account, this option can also be considered as Integration. However very high value assets are not normally converted at this stage with illegal funds; ● converting the illegal funds into money orders and/or checks; ● securities dealing: illegal funds are placed with securities firms which are used for buying bearer securities and other easily transferable instruments.
Layering	Layering is the second stage of ML. In this stage illegal funds or assets are moved, dispersed and disguised to conceal their illegal origin. There are numerous techniques and institutions that facilitate layering, including the following:

	• electronically moving funds from one country to another and dividing them into advanced financial options and or markets; • moving funds from one financial institution to another or within accounts at the same institution; • offshore banks: they accept deposits from non-resident individuals and corporations; • shell corporations: a shell corporation is a company that is formally established under applicable corporate laws but does not actually conduct a business. Instead, it is used to engage in fictitious transactions or hold accounts and assets to disguise their actual ownership; • trusts: they are legal arrangements for holding specified funds or assets for a specified purpose. These funds or assets are managed by a trustee for the benefit of a specified beneficiary or beneficiaries. Trusts can act as layering tools as they enable creation of false paper trails and transactions. The private nature of trusts makes them attractive to money launderers; • intermediaries: lawyers, accountants and other professionals may be used as intermediaries or middlemen between the illegal funds and the criminal. Professionals engage in transactions on behalf of a criminal Client who remains anonymous. These transactions may include use of shell corporations, fictitious records and complex paper trails.
Integration	Integration is the third stage of the ML process. In this stage, illegal funds are made to appear as though they are legitimate by turning those funds into normal everyday items or investments. Supplying apparent legitimacy to illicit wealth through the re-entry of the funds into the economy in what appears to be normal business or personal transactions. This stage entails using laundered proceeds in seemingly normal transactions to create the perception of legitimacy. The launderer, for instance, might choose to invest the funds in real estate, financial ventures or luxury assets. By the integration stage, it is exceedingly difficult to distinguish between legal and illegal wealth. This stage provides a launderer the opportunity to increase his wealth with the proceeds of crime. Integration is generally difficult to spot unless there are great disparities between a person's or company's legitimate employment, business or investment ventures and a person's wealth or a company's income or assets. There are various integration techniques, including the following: • import / export transactions: to bring illegal money into the criminal's country of residence, the domestic trading company will export goods to the foreign trading company on an over-invoiced basis. The illegal funds are remitted and reported as export earnings. The transaction can work in the reverse direction as well; • business recycling: legitimate businesses also serve as conduits for ML. Cash-intensive retail businesses, real estate, jewellers, and restaurants are some of the most traditional methods of ML. This technique combines the different stages of the ML process;

	• asset sales & purchases: this technique can be used directly by the criminal or in combination with shell corporations, corporate financings and other sophisticated means. The end result is that the criminal can treat the earnings from the transaction as legitimate profits from the sale of the real estate or other assets; • consultants: the use of consultants in ML schemes is quite common. The consultant could be fake. For example, the criminal could himself be the consultant. In this case, the criminal is channelling money back to himself. This money is declared as income from services performed and can be used as legitimate funds; • credit & debit cards: credit cards are an efficient way for launderers to integrate illegal money into the financial system. By maintaining an account in an offshore jurisdiction through which payments are made, the criminal ensures there is a limited financial trail that leads to his country of residence. Debit cards individuals first transfer illegal funds into an offshore account and then sign up for a debit card from the bank to utilize the funds; • corporate financings are typically combined with several other techniques, including the use of offshore banks, electronic funds transfers and shell corporations.

1.4. ML may not just involve wealth related to drug trafficking/TF. List of crimes identified by FATF as generators of criminal wealth also included but are not limited to:

- illegal arms sales;
- gun running;
- organized crime including drug trafficking and prostitution;
- embezzlement;
- smuggling (including movement of nuclear materials);
- counterfeiting (including making of imitation and copies of original products / goods);
- fraud, especially computer-supported fraud;
- benefiting from insider trading;
- bribery and kickbacks;
- tax evasion;
- under and over-invoicing of trade transactions;
- bogus trade transactions to launder money through round-tripping;
- facilitating illegal immigration;
- real estate transactions.

2. Terrorism Financing (TF)

2.1. In general, TF can be defined as any support, in any form, to terrorists or to those who encourage, plan, or engage in terrorism. A terrorist group, like any other criminal organization, builds and maintains an infrastructure to develop sources of funds and channel them to those who provide materials and or services to the terrorist organization.

2.2. Both terrorists and money launderers may use the same methods to move their money in ways to avoid detection, such as structuring payments to avoid reporting and use of underground banking or value transfer systems such as hawala, hundi, or fei-chien.

2.3. However, whereas funds destined for ML are derived from criminal activities, such as drug trafficking and fraud, TF may include funds from perfectly legitimate sources.

2.4. Concealment of funds used for terrorism is primarily designed to hide the purpose for which these funds are used, rather than their source. Terrorism funds may be used for operating expenses, including paying for food, transportation and rent, as well as for the actual material support of terrorist acts. Terrorists, similar to criminal enterprises, cover the secrecy of transactions regarding their destination and purpose.

Annex 2. Escalations

If any employee of the Company feels that they have found or witnessed suspicious activity, then such an employee shall submit an escalation to the Money Laundering Reporting Officer in writing explaining their concerns. An internal investigation shall be performed and if needed, STR will be filed to the FIU or the escalation will be closed providing an argument as to why the activity is not suspicious or does not warrant filing and STR to the FIU.

THE PURPOSE OF THE REPORT: THE PURPOSE OF THIS REPORT TO DRAW ATTENTION OF THE POSSIBLY SUSPICIOUS. ACTIVITY OF THE CLIENT. THE ACTIVITY WILL BE INVESTIGATE AND FURTHER DETAILS WILL BE ASKED IF REQUIRED.
FILLING INSTRUCTIONS: THIS REPORT NEEDS TO BE FILLED IN, SAVED AS PDF FILE AND SENT TO MONEY LAUNDERING REPORTING OFFICER AND THE MEMBER OF THE MANAGEMENT BOARD RESPONSIBLE FOR AML/CTF AS AN EMAIL ATTACHMENT.
TIPPING OFF: STAFF MEMBERS NEED TO TAKE INTO ACCOUNT THAT THEY ARE FORBIDDEN TO INFORM OR OTHERWISE DRAW ATTENTION OF THE CLIENT THAT ITS ACTIVITY IS UNDER INTERNAL INVESTIGATION. PLEASE ASK GUIDANCE FROM THE MEMBER OF THE MANAGEMENT BOARD RESPONSIBLE FOR AML/CTF AND/OR MONEY LAUNDERING REPORTING OFFICER ON HOW THIS SITUATION NEEDS TO BE HANDLED.