Policy on Anti-Money Laundering and combating the Financing of Criminal or Terrorist Acts

PART I - GENERAL

1. Introduction

This Policy on Anti-Money Laundering and combating the Financing of Criminal or Terrorist Acts ("**AML Policy**" or this "**Policy**") is adopted by SOLANIT OÜ, a company incorporated under the laws of Estonia, company number 14485024, with a registered office at Viru väljak 2-340, Kesklinna linnaosa, Tallinn, Harju maakond, 10111, Estonia , (the "**Company**" or "**SOLANIT**"), as of the date written above, to be executed and observed by the Company, its employees, affiliates and service providers.

The Company is committed to implement effective controls for the detection and prevention of illicit activities, which may be executed using its services, and to allocate substantial efforts and resources for that end.

We at SOLANIT believe that the adoption and adherence to this Policy will embed a compliance culture throughout the Company, provide solid and effective controls, and demonstrate that SOLANIT has committed itself and its resources to maintain and support the principles laid out within this Policy to uphold the Company's integrity, both internally and externally.

This Policy was written and adopted under the understanding that, as noted by authorities and organizations worldwide, the field of cryptographic assets, in which the Company is engaged, has an inherent level of risks of money laundering and terrorism financing ("**ML/TF**"). As such, this Policy includes, in addition to the procedures required under applicable laws, specific mechanisms and procedures aimed at mitigating such unique risks related to trading in crypto.

2. Framework

The Company is a provider of virtual currency exchange and wallet services, holding Financial Activity Licenses from the Estonian Financial Intelligence Unit ("**FIU**"), which is the Anti Money Laundering ("**AML**") authority in Estonia with the ability to grant, revoke and supervise Financial Activity Licenses.

The Company holds the following operating licenses, granted by the FIU:

License No. FVT000131 for providing services of exchanging a virtual currency against a fiat currency and for Providing a virtual currency wallet service.

Licensed financial activities providers are subject to AML and KYC (Know Your Client) requirements, set forth in the Estonian Money Laundering and Terrorist Financing Act (the "**Act**") and other legal guidelines given by the Estonian Minister of Finance (the "**Instruments**"). This Policy should be read in conjunction with these Instruments, in any conflict between the contents of this Policy and said Instruments, the latter shall prevail.

All sums denominated in this Policy in Euros (EUR) shall be read to include the equivalent amounts in any other currency or digital currency, as traded at the date of the relevant transaction.

3. AML/CTF Policy

This Policy aims to provide specific instructions on how personnel of the Company should perform actions, mandate internal procedures, and provide general guidelines for the instruction, control and training within the Company and its affiliates, in connection with the mitigation and handling of ML/TF risks.

This Policy shall act as binding guidelines to all relevant Company personnel, and all such personnel must be aware of, and adhere to, this Policy.

This Policy aims to present the Company's AML and KYC procedures:

- The Company's risk appetite;
- The criteria which are used to asses risk levels of business relationships and transactions;
- The criteria which are used to identify increased risk transactions;
- The essential features of transaction monitoring;
- The cases in which the Compliance Officer and Management Board shall be involved;
- The cases in which the designated Company personnel must report to the FIU;
- Providing AML training to relevant Company employees;
- The Company's policy regarding politically exposed persons;
- The methods which the Company's personnel uses to identify, limit and monitor increased risks;
- AML and KYC documents retention periods.

4. Responsibilities under this policy

a. Management Board

The Company's board of directors, which is the most senior body of management of the Company (the "**Board**"), shall bear the ultimate responsibility for the execution of the procedures under this Policy, and for amending it as necessary.

Member of the Board, as appointed by relevant Board decision, shall oversee the implementation of this policy, according to the AML/CTF requirements of the Instruments mentioned above (the "**AML Board Member**").

In addition to any other duty under this Policy, the Board shall be responsible for the following:

i. **Risk Appetite**
The Board shall establish the total ML/TF risks exposure level and types that the Company is prepared to assume in pursuing its business objectives ("**Risk Appetite**").

ii. **Annual Compliance Review**
The Board shall convene on an annual basis to review and assess the effectiveness of this Policy, the procedures taken under it, and the efficiency of the Compliance Function (as defined below) in general.

iii. **Supervision of AML Personnel**
The Board shall be responsible to supervise the Compliance Officer and other office holders listed below, and shall have the authority and responsibility for their appointment, removal and replacement.

b. Compliance Officer

The Board shall appoint a company official to head the Company's AML efforts, who shall be responsible for the effectiveness, adherence and compliance of this Policy, and serve as contact person between the Company and the FIU (the "**Compliance Officer**").

The Compliance Officer must be a qualified person, who has the education, professional suitability, abilities, personal qualities, experience and impeccable reputation required for the performance of these duties.

In addition to any other duty under this Policy, the Compliance Officer has the following responsibilities:

i. To ensure compliance with all duties under all applicable laws and regulations;
ii. To plan, supervise and document the ongoing basic and advanced training of all relevant personnel (Training Officer).
iii. To prepare, and subject to the Board's approval, any modification to this Policy.
iv. To act as contact to the FIU and the authorities.
v. To review possible ML/TF aspects of the development of new products or business practices, or from the use of new or enhanced technologies, assess their effect on the Foundation and provide recommendations to management.

vi. To prepare, and periodically review and update, the Risk Analysis.
vii. To present the Board the update on risks and controls.
viii. To submit Suspicious Activity Reports to the AML authorities.
ix. To prepare amendment to this Policy, when needed, and to present it to the Board for adoption.

c. Compliance Function

The compliance function is a department within the Foundation responsible for the implementation of this Policy and the mitigation of ML/TF risks in general, in its ongoing work process (the "**Compliance Function**"), subject to the direct supervision of the AML Officer.
The responsibilities of the Compliance Function shall include the following:

i. Executing AML related ongoing controls, including onboarding and ongoing customers activities;
ii. Advisory to senior management and business teams, covering current and expected level of Financial Crime risks.
iii. Implementation of this Policy and procedures cross the operational activities, verifying these procedures are up to date and aligned with the most updated regulation;
iv. Direct report to the Compliance Officer;
v. Supporting the compliance culture of the foundation, including training materials and training programs to employees in accordance with the risk exposure of their role;
vi. Implementation of Sanctions screening methods and alerts investigations;
vii. Supporting the governance activities and preparing the relevant Management Information to senior management to ensure appropriate decision making process;
viii. Responsible for engagement with local regulators upon need; and
ix. Supporting law enforcement enquiries and ensuring the relevant and accurate information is provided.

PART II – KYC PROCESS

Each person who applies to become a user of the Company's services ("**Client**") shall undergo an onboarding process comprised of a questionnaire, which shall include the Client's identification as well as certain additional information about the Client and its planned business relationship with the Company (the "**KYC Questionnaire**"), of an external review, flagging possible reputational ML/TF risks associated with the Client (the "**Screening**") and of an identification through documentation submitted by the Client (the "**Identification**") (together the "**KYC Process**").

The Company shall document and preserve any information and documents gathered in the KYC process, in a manner making it possible to respond fully and without unreasonable delay to relevant inquiries from competent authorities.

The KYC Process shall be accomplished following the KYC principle, according to which the operating profile, purpose of operation, beneficial owner of the Client and, if necessary, the source and origin of the funds used in the transaction and other similar information essential for the establishment of a business relationship shall be identified in addition to the identity of the Client itself. The KYC shall provide the necessary information for determining the Client's initial risk profile.

5. KYC Questionnaire

Any person applying to become a Client shall complete a short questionnaire to provide the Company with the basic information about itself, as the Company shall determine required considering the client's circumstances (the "**KYC Questionnaire**"), including regarding:

a. General Information

- Client's purpose and intent in the establishment of the business relationship;
- Client's anticipated size of transactions;

- Client's sources of income, fortune and assets;
- Client's occupation or field of activity;
- Client's permanent seat (place of residence/place of business);
- Client's main contracting partners (if relevant);
- Identity of the beneficial owner (if necessary);
- Client's telecommunication contact details;
- Any additional information which seems relevant in connection to a specific Client or group of Clients

b. For Natural Persons

- Full name;
- Personal identification code, or, if none, the date and place of birth;
- Whether the Client is himself a politically exposed person or related to one[1] ("**PEP**");

c. For Legal Entities

- Entity's name;
- Entity's registry code or registration number and date of registration;
- Information about the entity's legal form;
- Entity's passive legal capacity;
- Entity's legal representatives and those authorized to represent the entity before the Company names.

6. Screening

The details of the Client, as provided in the KYC Questionnaire, shall be screened against updated 'watchlists' (the "**Screening**"). The specific watchlists to be used for the Screening shall be determined by the Compliance Officer, and shall include, inter alia, sanction lists published by national and international authorities, lists of ML/TF suspicious persons published or held by third parties, and lists of identified PEPs.

7. Identification

Prior to entering into a business relationship, the Client must be identified by providing the Company with the information detailed in the KYC Questionnaire, backed with a copy of the following documents (the "**Identifying Documents**"):

a. Individuals

Any individual who must be identified under this Policy shall present one of the following identifying documents:

i. A document issued by the Republic of Estonia for digital identification of a person;
ii. Another electronic identification system with assurance level 'high' which has been added to the list[2] published in the Official Journal of the European Union based on Article 9 of Regulation (EC) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.08.2014, pp 73–114);
iii. Valid travel document issued in a foreign country; or-

[1] 'politically exposed person' means a natural person who is or who has been entrusted with prominent public functions including a head of State, head of government, minister and deputy or assistant minister; a member of parliament or of a similar legislative body, a member of a governing body of a political party, a member of a supreme court, a member of a court of auditors or of the board of a central bank; an ambassador, a chargé d'affaires and a high-ranking officer in the armed forces; a member of an administrative, management or supervisory body of a State-owned enterprise; a director, deputy director and member of the board or equivalent function of an international organisation, except middle-ranking or more junior officials;

[2] Available at: https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS

iv. Valid driver's license, that meets the requirements provided for in subsection 1 of § 4 of the Identity Documents Act[3].

b. Legal Entities

Any legal entity, which must be identified under this Policy, shall be identified using the following documents:

v. Registry card of the relevant register; and-
vi. Registration certificate of the relevant register; or-
vii. A document equal to a registration certificate (for instance, in countries where there is no national register, foundation documents certified by a notary are considered equivalent).

8. Establishing the Identity of Relevant Persons

Where the Client is a legal entity, the identities of the following persons (the "**Relevant Persons**") must be established, through the measures prescribed in subsection 7(a) above, in addition to the identity of the Client itself:

a. Beneficial Owners

The Client shall provide the Company with the information required to identify its beneficial owner. The following persons shall be considered as "beneficial owners", whose identity must be established in addition to the identity of the Client itself, for the purposes of this Policy:

i. A natural person who, taking advantage of their influence, makes a transaction, act, action, operation or step or otherwise exercises control over a transaction, act, action, operation or step or over another person and in whose interests or favor or on whose account a transaction or act, action, operation or step is made;
ii. Any person holding, alone or in concert, at least 25% of the voting rights or equity participation in the Client, or otherwise demonstrating effective control over the Client (each, a "**Controlling Person**");
iii. If any Controlling Person is not a natural person, any natural person who is to be regarded as controlling (in the sense given in paragraph (ii) above) is such a Controlling Person;
iv. If no Controlling Persons can be determined in accordance with paragraphs (ii) and (iii) above, the highest managing director or officer of the Client.

b. Representative

Where a person who is **not** the Client (e.g. signatory or representative) establishes the business relationship, the Client shall provide the Company with the following:

i. The identity of the natural person(s) who establish the business relationship (the "Representative"), in addition to that of the Client;
ii. Documents setting the Representative's authority (e.g. Power of Attorney, corporate resolution appointing the Representative) must be obtained and documented.

c. Where the business relationship is established by a trustee, nominee, protector, receiver, etc., all relevant documents establishing or confirming such person carrying out such a position must also be obtained and documented.

d. If there is any doubt regarding the authenticity or the legal force of a relationship referred to under this Section, further information, documents and/or proof should be obtained, and the business relationship shall not commence prior to such relationship being clarified.

Based on the information gathered via the KYC Process, the Company shall assemble an individual profile of the Client upon entry into a business relationship (the "**Client Profile**"). The Client Profile shall allow the Company to understand the Client's financial background, the origin of the Assets, and the purpose of

[3] The driver's license must contain the: name, photograph or facial image, signature or image of signature and date of birth or personal identification code of the holder.

the business relationship, as well as to check their plausibility in terms of legitimacy, or to identify circumstances that require particular clarification. Based on the Client Profile the Company shall preform a risk assessment, to determine the Client's risk profile and the necessary corresponding mitigating due diligence measures to be taken (the "**Risk Profile**").

PART III –DUE-DILIGENCE

The Company is committed to recognizing, assessing and understanding ML/TF risks it may face in connection with its Clients and their transactions, and to take appropriate measures to mitigate these risks using a risk-based approach.

The Company shall apply Client due diligence measures, to ensure the proper identification and verification of the Client or Client representatives participating in the transaction, as well as ongoing monitoring of business relationships, including transactions carried out during business relationships, regular verification of data used for identification, update of relevant documents, data or information and, when necessary, identification of the source and origins of funds used in transactions (the "**Due-Diligence**" or "**DD**" process).

Depending on the Client Risk Profile level and depending on whether the business relationship is an existing one or about to be established, the Company shall apply varying DD measures. For this reason, not all the procedures contained in this Part III shall be applicable to all Clients. Whenever the Company is unable to complete a DD measure, or doubt is arises during the application of a DD measure, the Company shall automatically raise the Client's Risk Profile Level, and apply a more stringent DD measure.

DD shall include the following procedures:

9. Risk Assessment

When determining the risk profile and the corresponding due diligence mitigating measures, the Company shall take account, when relevant, the information detailed in subsection (a) and the risk assessment detailed in subsection (b):

a. Information affecting the risk profile

- Provisions of the National Risk Assessment, as published on the website of the Ministry of Finance;
- Information regarding the nature of the business relationship and/or occasional transaction, as gathered in the KYC Process;
- The volume of the property deposited by the customer or the proprietary volume of the transaction or of transactions made during a professional act;
- The estimated duration of the business relationship;

b. Risk assessment

The risk assessment shall take into account the following risk categories, the probability and consequences of their realization and the probability of an increase in the risk:

i. Client associated risks, whose factors arise from the person or client participating in a transaction. These factors may include:

- The legal form, management structure and field of activity of the client, including whether it is a trust fund, civil law partnership or another similar contractual legal entity or a legal person with bearer shares;
- Whether the client is a PEP;
- Whether the client is a Shell Bank;
- Whether the client is represented by a legal person;

- Whether a third party (individual) is the beneficial owner;
- Whether the identity of the beneficial owner is impeded by complex and non-transparent ownership relations;
- The residency of the client, including whether the client is registered in a low tax rate jurisdiction;
- Whether the client is included in international sanctions lists4;
- Circumstances (including those identified in the course of a prior business relationship) resulting from the experience of communicating with the client, its business partners, owners, representatives and any other such persons;
- Whether the origin of the client's assets or the source and origin of the funds used for a transaction can be easily identified;
- The type and characteristics of the client's business;
- The possibility of classifying the client as a "typical client"; and-
- Problems during the client's identification procedures.

ii. **Transaction associated risks**, whose factors result from the Client's economic activities or the exposure of a specific product or service to potential money laundering risks. These factors may include:
- The transaction involves currency exchange or purchase of precious metals;
- The transaction involves a private bank;
- The transaction involves alternative payment methods;
- The transaction involves gambling;
- The transaction involves rarities or exclusive goods;
- The transaction involves innovations;
- The transaction involves commercials; and-
- The transaction involves company establishment or management.

iii. **Country or geographical associated risks**, whose factors arise from differences in the legal environment of various countries, these factors may include:
- Whether the transaction involves low tax rate jurisdictions, entailing a company registered to such jurisdiction or services provided at such jurisdictions[5];
- Whether the jurisdictions involved apply legal provisions that are in compliance with the international standards of AML/CTF[6];
- Whether the transaction involves a jurisdiction with a high crime rate (including drug-related crime rate);
- Whether the transaction involves a jurisdiction that is included in international sanction lists; and -
- Whether the transaction involves a jurisdiction with high levels of corruption according to the Corruption Perceptions Index ("CPI") published by Transparency International.

iv. **Interface associated risks**, whose factors arise from the channels (mainly the Internet) through which the business relationship is established, and the transactions are carried out, these factors may include:
- Whether the client is identified face-to-face;

[4] The Consolidated list of persons, groups and entities subject to EU financial sanctions is available at: https://webgate.ec.europa.eu/europeaid/fsd/fsf

[5] A List of countries that are **NOT** regarded as low tax rate countries (established by Estonian Ministry of Finance) can be found here: https://www.emta.ee/et/ariklient/tulud-kulud-kaive-kasum/mitteresidendi-eesti-tulu-maksustamine/nimekiri-territooriumidest

[6] A list of high risk non AML/CTF cooperative countries is available at: http://www.fatf-gafi.org/countries/#high-risk

- Whether the channel facilitates anonymity; and-
- Whether the channel facilitates third party funding.

10. Risk profile

The conducted risk assessment shall result in a risk profile, identified through the risk factors mentioned above, and according to the following scale:

a. Low Risk Profile: risk is considered low when there are no influential risk factors in any category. The client and the transaction can be described as "typical" and transparent, and there is no suspicion that the combination of risk factors may lead to the risk of ML/TF.

b. Medium Risk Profile: risk is considered medium when there are one or more risk factors that differ from the sphere of the "typical" client, but the transaction itself is clear (i.e. there are no risk factors in the transaction associated risks category). At the same time, there is no suspicions that a combination of the risk factors may indicate of ML/TF;

c. High Risk Profile: risk is considered high when there are multiple risk factors and the transaction itself is not clear. The combination of these factors casts doubt on the transparency of the client's identity and transactions, indicating of ML/TF.

- Any Client identified as a PEP shall be classified as High Risk Profile;

Examples of risk indicators applicable to the above categorization is attached hereto as **Annex 1.**

The Company shall document the determination of the risk profile, update it and make the data available to competent authorities, if necessary.

11. Verification

The Company shall verify the identity of the Client and, in the case of legal entities, the Client's representatives and beneficial owners, as provided through the KYC Questionnaire and Identification Documents, applying the following measures:

a. Individuals

i. **Where the Client's Risk Profile is low -** A document submitted to the Company for identification shall be assessed by the Compliance Function as follows:
   - Validity of the document based on the expiry date;
   - The outward likeness and age of the person match the appearance of the person represented on the document;
   - When relevant, the personal identification code matches the gender and age of the submitter;

ii. **Where the Client's Risk Profile is medium** – in addition to the measures described above, The Compliance Officer shall describe and apply additional verification measures, which may include:
   - Additional documents, data or information originating from a reliable and independent source; or-
   - Verification on the basis of trust services;

iii. **Where the Client's Risk Profile is high** – in addition to the measures described above, The Compliance Officer shall obtain the further verification measures, which shall be approved by the AML Board Member, these may include:
   - Additional documents, data or information originating from a reliable and independent source;
   - A notarized or officially authenticated copy of the Identification Documents;

b. Legal Entities

i. **Where the Client's Risk Profile is low -** A document submitted to the Company for identification shall be assessed by the Compliance Function by accessing the relevant register electronic database;

ii. **Where the Client's Risk Profile is medium** – in addition to the measures described above, The Compliance Officer shall describe and apply additional verification measures, which may include:
- Obtaining additional documents, data or information originating from a reliable and independent source;
- Verification on the basis of trust services;

iii. **Where the Client's Risk Profile is high** – in addition to the measures described above, The Compliance Officer shall obtain the further verification measures, which shall be approved by the AML Board Member, these may include:
- Additional documents, data or information originating from a reliable and independent source;
- Obtaining corporate documents certified or authenticated by a notary or officially;

c. Verification of the Identity of Beneficial Owners

The Company shall verify the identity of the Beneficial Owner, applying the following measures:

i. Where the Client is a company listed on a regulated market, which is subject to disclosure obligations that establish requirements for ensuring sufficient transparency regarding the beneficial owner – no additional verification measures shall be required;

ii. **Where the Client's Risk Profile is low -** a written statement must be obtained, confirming such persons being all of the Controlling Persons (or highest managing director or officer, in the case of 10(iv above) of the Client (the "**Controlling Persons Statement**"). The Controlling Persons Statement must be dated and signed by the person authorized by the Client to do so, on behalf of the Client and approved by the Compliance Function;

iii. **Where the Client's Risk Profile is Medium** – in addition to the measure detailed in subsection (b), enquiries to the respective registers shall be made and additional documentation identifying the Controlling Persons must be obtained. The additional documentation may include company records or annual reports clearly identifying the Controlling Persons, as approved by the Compliance Officer ;

iv. **Where the Client's Risk Profile is High** – in addition to the measures detailed in subsection (b)-(c) above, the Company shall obtain additional verification from credible sources. This verification may include information received in a format reproducible in writing from a credit institution ("**CI**") registered in the European Economic Area or in an equivalent third country or a branch thereof. The additional verification shall be brought before and approved by the AML Board Member.

Whenever the Company establishes that the identification of a Client is insufficient, enhanced verification measures shall be applied.

12. Clarifications and Collection of Additional Information

For any risk indicator identified by the Company during the performance of the procedures described above, additional details and information shall be collected for the purpose of understanding and mitigating such risks. As prescribed by the competent Company function (determined in accordance with the Client's risk level), the following measures shall be applied in connection with <u>each</u> risk factor identified:

a. Where the Client's Risk Profile is Low – Compliance Function shall contact the Client for further clarifications, provision of documentation and/or proof;

b. **Where the Client's Risk Profile is Medium** – in addition to the measure described above, The Compliance Function shall conduct a verification of the further information received from the Client through a reliable and independent source of information;
c. **Where the Client's Risk Profile is High** – in addition to the measures described above, the Compliance Function shall conduct a thorough review of each Risk Factor and additional information received regarding it, which may include its verification through an additional second reliable and independent source of information as well as requiring further documentation from the Client, and submit the same for the review and approval of the Compliance Officer.
    - For example: in the case of a Client's High Risk Profile due to doubts regarding its source of funds, the Compliance Function may require the Client to submit bank confirmations and tax reports, conduct a verification of the documents filed, and review the plausibility of the Client's funds in light of the additional information gathered. If the Compliance Function is convinced that the documents provided are complete and accurate, and provide sufficient comfort regarding the legitimacy of the Client's funds, a report of the same shall be submitted to the approval of the Compliance Officer.
d. **Where the Client's is a PEP** – in addition to the measures described above, a thorough review into the Client's source of funds (regardless of any additional risk indicator applicable), and gathering of relevant documentation shall be conducted by the Compliance Officer, the results of which shall be brought for the final approval of the AML Board member.

13. Approval of Client Business Relationship

Upon the completion of the DD measures described above, the business relationship may be approved by the corresponding authority within the Company and established, as follows:

a. **Where the Client's Risk Profile is Low** – The Compliance Function shall review the information gathered in the DD process and approve the establishment of a business relationship;
b. **Where the Client's Risk Profile is Medium** – The Compliance Officer shall review the information gathered in the DD process and approve the establishment of a business relationship;
c. **Where the Client's Risk Profile is High** – The AML Board Member shall review the information gathered in the DD process and approve the establishment of a business relationship;

PART IV – ONGOING AML REQUIREMENTS

14. Ongoing Monitoring

a. Ongoing Monitoring of Transactions

Every transaction which is undertaken by a Client with the Company shall be electronically monitored and reviewed to ensure that they are in concert with the Client's initial declared scope and purpose for the establishment of the business relationship and coherent with the Client's Risk Profile and transactional history (the "**IT Monitoring**"). Said monitoring shall identify transactions which should be more thoroughly examined, based, among others, on frequency of transactions, forming or breaking of any pattern of behavior, size of transaction, etc., taking into account the profile of the specific Client, and the observed characteristics of relevant groups of Clients.

Where a transaction is flagged as unusual or suspicious of ML/TF, the Compliance Function shall manually review the findings, assess the risks and operate according to its findings. After the aforementioned review is undertaken, the Risk Function shall document the transaction and the results of its review in the Client's AML File.

If the Risk Function determines that a transaction is suspicious of ML/TF, it shall provide a Report of Suspicion as detailed below.

b. Ongoing Monitoring of Business Relationships

i. All Business Relationships

A. **Screening**

The details of Clients (as well as those of their Relevant Persons) shall undergo a Screening, at least:

i) **Where the Client's Risk Profile is Low** – every 3 months;

ii) **Where the Client's Risk Profile is Medium** – every 2 months;

iii) **Where the Client's Risk Profile is High** – every month;

B. The IT Monitoring procedures shall be conducted on an ongoing basis, identifying not only suspicious transactions, but also other issues related to the Clients and the business relationships which should raise awareness. Once such an issue is flagged by the IT Monitoring, the Compliance Function shall immediately review it manually.

C. The Compliance Function shall periodically review all existing business relationship to identify any changes which seem to have occurred in connection with the Clients, conduct a more overreaching review of the different transactions made with it over the entire business relationship, and identify any unusual or suspicious details which might have been missed in the review of specific transactions as described above.
Such reviews shall take place at least:

- For Low Risk Profile Clients – once every 18 months;
- For Medium Risk Profile Clients – once every 12 months;
- For High Risk Profile Clients – once every 6 months;

D. The Compliance Officer shall perform routine sampling of the AML Files, reviewing the appropriateness and completeness of such Files and the processes documented therein.

ii. Medium Risk Profile Business Relationships

In addition to the reviews undertaken in accordance with paragraph (i) above, the Compliance Officer shall review, at least once per year, each business relationship of Medium Risk Profile Clients.

iii. High Risk Profile Business Relationships

In addition to the reviews undertaken in accordance with paragraphs (i) and (ii) above, the AML Board Member shall annually review and decide on the continuation of any High Risk Profile business relationship.

c. Identifying 'Suspicious' Business Relationships/Transactions

The reviews described above shall aim at detecting:

i. any discrepancies between the information previously gathered (as documented in the Client's AML File) and any information which is currently known or is available to the Company (e.g. any updates or changes which have occurred in the Client's details);

ii. any discrepancies between the Client Profile and the transactions undertaken by it (e.g. transactions which do not seem to match the Client's financial status or expected scope of business); and

iii. any other suspicious behaviour or pattern (e.g. transactions with no visible business logic, frequent purchase/sell/transfer of funds).

If any of the above is detected by an employee, whether as part of a routine review by the Compliance Function, or by any other means, it shall immediately be reported to the Compliance Officer.

An employee does not need to have evidence that money laundering is taking place in order to have a suspicion of such money laundering. All employees will be encouraged to seek advice from their manager and/or the Compliance Officer if they have any queries.

d. Change in Risk Levels

If, at any time after the establishment of the business relationship, there is a reason to alter the Client's Risk Level, this issue shall be brought before the Compliance Officer, who may decide on this issue and alter such Risk Level, or bring it before the Board to do the same.
Such reasons may include, *inter alia*:

- New information regarding the Client that has come up during Screening;
- Suspicion regarding the Client has been rising by one of the Company's employees;
- The Company becomes aware of any new and relevant information.

e. Inactive Business Relationship

Where a Client does not perform any transaction with the Company for a period exceeding 6 months, such Client will become an 'inactive client' and the Company will cease performing all ongoing measures described above. Where an inactive Client wishes to perform another transaction, the Company shall perform the necessary reviews to revalidate its status before completing such transaction.

15. Registration and Storage of Data

a. The Company shall register all the Client's information obtained in the KYC Process and DD procedures in the Company's Clients database, including all data regarding Company decisions on approval or refusal of establishment of business relationship or a transaction.

b. The respective data shall be stored in a format reproducible in writing and, if required, shall be made accessible by all appropriate staff of the Company.

c. Documents which serve as the basis for the identification of a Client or Client representative, and documents serving for the establishment of a business relationship shall be kept and stored by the Company for at least five (5) years following the termination of the business relationship, or as otherwise required by applicable law.

PART V - REPORTING SUSPICIOUS BUSINESS RELATIONSHIPS/TRANSACTION

16. Report to the Compliance Officer

Internal reporting of any suspicious matters in connection with this Policy shall be made immediately by the individual having such suspicions (regardless of whether or not such individual part of the Compliance Function) to the Compliance Officer.

The Compliance Officer shall analyze the content of the information received and forward the respective information to the AML Board Member.

a. Evaluation of Suspicion

The Compliance Officer, upon receiving a report (or in any other manner becoming aware of any suspicion of ML/TF), shall immediately review such suspicion, evaluate its merits, and conclude what actions shall be taken in connection therewith. In doing so, the Compliance Officer may consult the Compliance Function, the employee who reported the suspicion, the Board, or any other person within the Company.

The actions which the Compliance Officer may decide to be taken may vary depending on the circumstances, and include any action mentioned in this Policy. These include, but are not limited to:

i. no-action;
ii. instructing the Compliance Function to conduct further review;
iii. reclassification of the Risk Level of the business relationship;
iv. immediate termination of negotiations aimed at establishing the business relationship;
v. reporting to the AML Board Member; and
vi. reporting to authorities, as further described below.

17. Report to the FIU

The Compliance Officer is responsible for determining when a report to the FIU is to be made, and for making the report.

The FIU shall be notified of any suspicious and unusual transactions, including such where the financial obligation exceeds 32.000 Euros or an equivalent amount in another currency is performed in cash, regardless of whether the transaction is made in a single payment or several related payments over the course of a year.

The Client who is reported to the FIU as being suspicious, may not be informed of the same. It is also prohibited to inform any third persons, including other employees, of the fact that information has been reported to the FIU, and the content of the reported information, except for the AML Board Member/Compliance Officer.

a. Duty to Report

A report to the FIU **must** be filed if the Company knows or has reasonable grounds to suspect that assets involved (or which are expected to be involved) in the business relationship, not later than within two (2) business days after discovering any activities or circumstances or arising of suspicion:

i. Are the proceeds of a felony or of an aggravated tax misdemeanor;
ii. Are connected to money laundering or to a criminal organisation which pursues the objective of committing crimes of violence or which aims at financial gain by criminal means;
iii. Serve the financing of terrorism;
iv. Are subject to the power of disposal of a criminal organisation; or
v. Are related to persons contained on sanction lists.

The abovementioned duty to report to the FIU arises whether such knowledge or suspicion arises **before or after a business relationship is established** (i.e. whether the Company refuses to establish the relationship or establishes it and gain such knowledge or suspicion at a later date).
A report to the FIU must also be made immediately if any other competent authority, forwards to the Company in any manner the details of a person which they consider to be involved in unlawful activities of any kind, and the Company finds that the information regarding such person matched or is very similar to that of a Client, its controlling person, beneficial owner of the assets or authorized signatory of a business relationship or transaction. In any such event, the Company must immediately freeze the assets entrusted to it which relate to the report, until it receives an order from the competent prosecution authority, but at the most five (5) working days from the time at which the relevant report was filed with the FIU.

PART VI – OTHER REQUIREMENTS

18. Training

All Company employees must undergo AML training in a manner, scope and frequency appropriate to their role in the Company.

Such training shall be conducted, monitored and documented as prescribed by the Compliance Officer, and reviewed by the AML Board Member on an annual basis, together with this Policy.

The Compliance Officer is responsible for ensuring that all employees are aware of their responsibilities under this Policy, including applicable laws and regulations, and are familiar with the procedures of identifying and reporting suspicious transactions, business relationships or activities. All employees must be aware that non-compliance with this matter may result in legal action, including criminal action, being taken against them.

Employees involved with any interaction with customers, operational processes supporting on boarding, customer activity or execution of customers activities will not be allowed to conduct their roles prior to completion of basic AML training.

19. Internal Review and Amendment of this Policy

Compliance with this Policy shall be inspected at least once a year by the Compliance Officer and presented to the Board in a written format. The report on the results of the inspection concerning the compliance with the measures for prevention of ML/TF shall set out the following information:

- date of the inspection;
- name and position of the person conducting the inspection;
- purpose and description of the inspection;
- analysis of the inspection results, or the conclusions drawn on the basis of the inspection.

If the inspection reveals any deficiencies in this Policy or their implementation, the report shall set out the measures to be applied to remedy the deficiencies, as well as the respective time schedule and the time of a follow-up inspection.

If a follow-up inspection is carried out, the results of the follow-up inspection shall be added to the inspection report, which shall state the list of measures to remedy any deficiencies discovered in the course of the follow-up inspection, and the time actually spent on remedying the same. The inspection report shall be presented to the AML Board Member, who shall decide on taking measures to remedy any deficiencies discovered.

Annex 1: Examples of indicators for risk categorization

1. **The following is deemed a situation reducing risks relating to the customer type**:
   i. The Client is a company listed on a regulated market, which is subject to disclosure obligations that establish requirements for ensuring sufficient transparency regarding the beneficial owner;
   ii. The Client is a legal person governed by public law established in Estonia;
   iii. The Client is a governmental authority or another authority performing public functions in Estonia or a contracting state of the European Economic Area;
   iv. The Client is an institution of the European Union;
   v. The Client is a credit institution or financial institution acting on its own behalf or a credit institution or financial institution located in a contracting state of the European Economic Area or a third country, which in its country of location is subject to requirements equal to those established in Directive (EU) 2015/849 of the European Parliament and of the Council and subject to state supervision;
   vi. The Client is a person who is a resident of a country or geographic area having the characteristics specified bellow.
2. **The following may be deemed a factor reducing geographic risks**:
   i. A contracting state of the European Economic Area;
   ii. A third country that has effective AML/CFT systems;
   iii. A third country where, according to credible sources, the level of corruption and other criminal activity is low;
   iv. A third country where, according to credible sources such as mutual evaluations, reports or published follow-up reports, AML/CFT requirements that are in accordance with the updated recommendations of the Financial Action Task Force (FATF), and where the requirements are effectively implemented.
3. **The following is deemed a situation increasing risks related to the customer as a person**:
   i. The business relationship foundations based on unusual factors, including in the event of complex and unusually large transactions and unusual transaction patterns that do not have a reasonable, clear economic or lawful purpose or that are not characteristic of the given business specifics;
   ii. The Client is a resident of a higher-risk geographic area as listed below;
   iii. The Client is a legal person or a legal arrangement, which is engaged in holding personal assets;
   iv. The Client is a cash-intensive business;
   v. The Client is a company that has nominee shareholders or bearer shares or a company whose affiliate has nominee shareholders or bearer shares;
   vi. The ownership structure of the Client's company appears unusual or excessively complex, given the nature of the company's business.
4. **The following is deemed a situation increasing risks related to the product, service, transaction or delivery channel**:
   i. Private banking;
   ii. Provision of a product or making or mediating of a transaction that might favour anonymity;
   iii. Payments received from unknown or unassociated third parties;
5. **Situation where the Client, a person involved in the transaction or the transaction itself is connected with a following country or jurisdiction is deemed as a situation increasing the geographical risk**:
   i. Jurisdiction that, according to credible sources such as mutual evaluations, detailed evaluation reports or published follow-up reports, has not established effective AML/CFT systems;
   ii. Jurisdiction that, according to credible sources, has significant levels of corruption or other criminal activity;
   iii. Jurisdiction that is subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations;
   iv. Jurisdiction that provides funding or support for terrorist activities, or that has designated terrorist organizations operating within their country, as identified by the European Union or the United Nations.

V4-25.11.2020