Approved by the decision of the Managing Partner of EXFRAME OU dated March 01, 2021.

The document becomes effective: 07.03.2021
The document is valid from: 10.03.2021

RULES OF PROCEDURE
AND BY-LAWS

to perform obligations to counter money laundering and terrorism financing
within the EXFRAME OU Company

I. General provisions

1.1. The EXFRAME OU (hereinafter referred to as the "Service provider") is the obliged (designated) person based on the following Acts:
Money Laundering and Terrorist Financing Prevention Act and Republic of Estonian Money Laundering and Terrorist Financing Risk Assessment 2015 (AML/CTF) that specify that the AML/CTF is applied to economic activities of financial institutions, and that a financial institution consider the following as in the AML/CTF actions:
- service offer on virtual currency exchange for money;
- service offer to act as the wallet for virtual currency.

1.2. This practical instruction specifies internal security measures of the Service provider to perform obligations for anti-money laundering and counter-terrorism financing compliance and to detect suspicious and unusual deals (transactions).
1.3. Employees of the Service provider and of its business partners should be aware of and strictly comply with requirements specified in Criminal Justice Money Laundering and Terrorist Financing) Acts; in instructions issued by the Anti-Money Laundering Compliance Unit to detect signs of transactions suspicious for money laundering and terrorism financing, as well as to detect unusual transactions.
1.4. Employees of the Service provider and employees of its business partners who are directly involved in personal identification, are obliged to personally read and understand changes (amendments) in laws and other legal acts.
1.5. The Service provider's management shall be obliged to inform its personnel with this practical instruction. The Service provider's employees shall be obliged to acknowledge that they have read and understood this instruction by personal signature.
1.6. Employees of the Service provider shall be personally responsible to comply with requirements of Criminal Justice (Money Laundering and Terrorist Financing) Act as per procedure as established by law.
1.7. The relevance of procedural rules shall be regularly checked; they shall be supplemented and updated as necessary, but at least once a year.

II. Terms

2.1. **Offering the virtual currency exchange service for money** is the virtual currency represented as the value in digital expression that may be transferred, stored or sold through e-services on digital basis, and that is accepted by individuals or legal entities as the means of payment, but that is not the legal means of payment of any state or monetary means as it is understood as per the clause 25 of Article 4 of the Directive EU on Payment Services (PSD2), or the payment instrument or payment deal as per clauses "k" and "l" of Article 3 of the same Directive.
2.2. **Offering the virtual currency wallet service** is the creation or storage of the client encrypted keys within the service that may be used to store, deposit and transfer virtual currencies.
2.3. **Service provider** is a legal entity being a service provider that, in the course of its economic activity, allows the client to make the virtual currency exchange for money and use the wallet service

for virtual currency for fee (service charge) based on terms of Transaction concluded between the Service provider and the Client.

2.4. **Client** is a capable physical person and/or a legal entity with which the Service provider maintains business relations and whose identity is ascertained as per the identity paper prior to sign a transaction between the Service provider or the partner of the Service provider in line with requirements of the AML/CTF, internal procedural rules of the corporate Commercial Association and its bylaws.

2.5. **Employee** is a Service provider whose task is to build and maintain business relations, to process data relating to transactions, to identify and assess risks, and to minimize and manage risks.

2.6. **Invoice** is a document with services of transaction listed and the amount payable.

2.7. **Contact person** is a representative of the Service provider who is the contact person for the Anti-Money Laundering Compliance Unit and who regulates and controls enforcement of measures to resist money laundering and terrorism financing within business activities held by the Service provider. The contact person shall be responsible for performance of obligations that arise based on International Sanctions Act. The Board/Managing Partner of the Service provider is involved in tasks of a contact person until it is assigned.

2.8. **Business relations** are relations of the authorized person (under the meaning of these procedural rules) arising at conclusion of a long-term transaction as part of economic or professional activity, or those not based on long-term transaction, but at which, during the contact building, certain duration is reasonably expected, and during which the authorized person repeatedly makes individual deals as part of economic, professional or official activity.

2.9. **Money laundering** is measures committed against the property obtained from the criminal activity, or the property obtained in lieu of such property:

1) true essence, origin, location, way of disposal, transfer, ownership or other rights related to the property concealed or kept in secret;

2) conversion, transfer, acquisition, possession or disposal for the purpose to conceal or keep in secret the illicit origin of this property, or for the purpose to render assistance to a person involved in criminal activity so that it may avoid legal consequences of its actions.

3) Money-laundering applies to cases where the criminal activity, resulting in the property obtained to be used for money-laundering procedure, took place within the territory of another state.

2.10. **Financing of terrorism** is asset allocation or collection to plan or take actions considered as terrorism under the meaning of the Penitentiary code, or to finance terrorist communities, or be aware that such funds are used for aforementioned purposes.

2.11. **Anti-Money Laundering Compliance Unit (hereinafter referred to as AMLCU)** is an independent structural unit of the Department of Justice that supervises and applies official enforcement based on and in a manner as prescribed by law. Postal address: Pärnu mnt 139, Tallinn, 15060; E-mail: ppa@politsei.ee

2.12. **International financial sanctions** are those decided to be put into effect by the European Union, by the United Nations (UN), another international organization or the Government of Estonia. It relates to measures of non-military nature that, wholly or in part, prevent that the subject of international financial sanctions uses and disposes money and that such funds are transferred to possession thereof.

2.13. **A risk bearing state** is a state of concern in terms of anti-terrorism, or a region of higher risk terrorism, or a country of high risk for terrorism where international sanctions are applied, or those known for the high level of corruption, or a state with insufficient regulatory measures to counteract money laundering, or there is another source of higher risk.

2.14. **Politically exposed person (hereinafter referred to as the "PEP")** is an individual who is in charge, or was in charge, for important tasks of public authority (including. the head of state, head of government, a minister and the deputy or assistant minister, member of Parliament or of a legislative body similar to the parliament, member of the managing body of the party, member of the Supreme and State Court, member of the State Authority Board or of the Central Bank of the country,ambassador, solicitor and senior officer of armed forces, member of the Board, supervisory or administrative body of a state-owned company, the head, the deputy and a member of the managing

authority of any international organization or a person who performs similar functions and who do not hold the status of a middle- or low management official.

- **Local politically exposed person** - a natural person who performs or used to perform important tasks of public authority, including the head of state, head of government, a minister and a deputy or assistant minister, member of the parliament ot any legislative body similar to the parliament, a member of the managing body of a party, member of the Supreme and State courts, ember of the Board for the State control or Central Bank of the country, an ambassador, a solicitor and a senior military forces officer, member of the board, of supervising or administrative body of a state-owned company, a head, a deputy and a member of the managing body of an international organization or a person who performs the similar tasks and who does not hold a status of the middle- or low management official who performs or used to perform important tasks of public authority in Estonia, in any other state party to the Agreement on European Economic Space or at the European Union Body.
- **A member of the PEP's family** is a spouse of a politically exposed or of a local politically exposed person /partner equal to a spouse of that person, his/her child and spouse or partner of the child equal to the spouse, a parent of that person.
- **A close PEP's employee** is an individual who is known to be a factual beneficiary or joint owner of a legal entity or of legal branch along with the politically exposed person or local politically exposed person, or that who has close business relationship with a politically exposed person, or local politically exposed person, or a natural person who is the sole beneficiary of that legal entity or of legal branch who is known to be de facto established in favor of a politically exposed or a local politically exposed person.

2.15. **Actual beneficiary** is a natural person who, using its authority, supervises the transaction, deal or the other person, and in whose interest, in whose favor or for whose expense a deal or a transaction is concluded, including a person who owns at least 25% shares, equity interests, company's votes or property, or that otherwise controls the management of a legal entity.

III. A person's identity when making transactions and creating business relations

3.1. The Service provider shall be obliged to identify each client's identity when building business relationships and making a deal.

3.2. Considering requirement of the clause 3.1, an employee applies the following procedural rules any time prior to make a deal with a client or build business relationships;

3.2.1. ascertains a person's identity and verifies its identity based on the documents valid travel document issued by a foreign state, or a driver's license.

3.2.2. makes a copy/electronic copy of the page with personal data and the photo from the identity paper submitted to ascertain the identity;

3.2.3. when ascertaining person's identity and verifying the information submitted, the following data is recorded:

- first and last name;
- personal code, if no any code, the date of birth and place of birth;
- title and number of the document used for identification and verification of identity, date of its issuance and name of the issuing authority;
- residence address of the person and his specialty, or sphere of activity;
- purpose of transaction and date of the transaction;
- if a client is a natural person of another state-member to the agreement on European economic space or a third country, the employee shall register the information on whether or not the person performs significant tasks of public authority, whether it is a close employee or a member of the family of the executor of significant tasks of public authority;

3.3. The following documents may be used as the basis to identify a natural person:

- Documents issued based on Estonian legislation: Identity card; e-identity card; residence permit card; diplomatic passport; seaman's service book; alien's passport; temporary traffic document; refugee's travel document; naval certificate; certificate of repatriation; permit for repatriation;

- valid travel document or driver's license issued by a foreign country if the document includes the user's first and last name, a photo or image of the person, signature or image of the signature, as well as the date of birth or personal code.

3.4. During identification, the employee should assess the authenticity of the document submitted based on the following circumstances[1]:

- validity of the document and its compliance with requirements of the Act of Identity Document;
- physical resemblance of the person with appearance in the photo in the document and compliance of the age of the person to data contained in the document.

3.5. When making transactions with a politically exposed person of another member state of the European Economic Area (hereinafter referred to as the "EEA") or a third country, the employee shall be governed by provisions of AML/CTF.

3.6. If the person identification is suspicious to act in the name other than its name, or at the expense of other person, the employee identifies the person on behalf of or at the expense of which the first person acts. The actual beneficiary may be suspected to arise, first of all, if diligence actions are taken where it feels as if an individual declines to build business relationship or to make a deal. In such a case, the person who supervises this individual should be considered the actual beneficiary of the individual.

3.7. Knowledge of the client by name and his publicity shall not be the ground for non-compliance with the rule on person identification as established by law.

3.8. If necessary, the employee may ask to verify the authenticity of information submitted by the client at his handwritten signature.

3.9. The employee of the Service provider shall be prohibited to make a transaction:

- with a person who refuses to submit the data referred to in the clause 3.2;
- If the client fails to submit the required documents and appropriate data;
- If, based on documents submitted, the employee suspects that the case may be money laundering or terrorist financing;
- If the person, on behalf of or at the expense of which the other person acts, is not identifiable, or if a fake person is suspected.

3.10. Cases referred to in the clause 3.9. of this instruction should be immediately communicated to the contact person of the Anti-Money Laundering Compliance Unit and as much data of the client should be recorded as possible that may help identify the client later.

3.11. Person identity is performed while staying at the same place with the person which identity is ascertained, or the identity assertion procedure may require a document certified by notary or acknowledged by notary or the authorized body, or other information from the reliable and independent source.

3.12. If the employee has doubts about the client's identity, the former should require for an additional document with a photo to ascertain the identity that allows to verify the correctness of the person identification. If a falsified document is suspected, it is recommended that it is kept, a police is called and the document that arises suspicion is submitted to the former. In this case, Anti-Money Laundering Compliance Unit should be reported on that.

[1] When checking documents from the employee of the Service provider, no expert knowledge of falsified (fake) documents is required, but the employee is prohibited to neglect apparent falsification signs.

IV. Politically exposed persons

4.1 The authorized person shall establish internal procedures to take decisions on whether the potential client or actual beneficiary of the client is a politically exposed person (including that of domestic significance) in the other state-member to the agreement on European economic space or a third country, or a person who performs or has performed important tasks for international organizations.
4.2 The authorized person shall identify close employees and family members of politically exposed persons only if their link to the executor of important tasks of state authority is known to the public, or if the authorized person has grounds to believe that this link is available.
4.2.1 In terms of politically exposed persons, the authorized person shall apply, apart from appropriate verification measures, additional measures, in particular:
- to request the information needed from the client, including the case to take appropriate measures to define sources of property and funds used for business relationships or transaction;

To verify data or make a request to relevant databases[2] or public databases[3]; or on the site https://www2.politsei.ee/et/organisatsioon/rahapesu/;
- to make a request or verify the data on websites of relevant supervisory authorities or institutions in the country where the customer or person is located.

4.2.2 The decision to build business relationships with a politically exposed person shall be taken by the board/Managing Partner of the authorized person or person(s) authorized by the Board/Managing Partner If business relationships with the client are built and the client or the actual beneficiary shall be apolitically exposed person consequently under the meaning of clause 2.1 of this instruction, the Board/Managing Partner (or persons authorized by the Board/Managing Partner) should be reported on that.
4.2.3 The authorized person shall arrange the regular strengthened control of business relations concluded with a politically exposed person, except for cases specified in legal acts.
4.2.4 Also, the authorized person should take care of regular control even after the politically exposed person terminates its activity if, in opinion of the authorized person, the specified person still carries a higher risk.
4.2.5 Under situations when a person who is involved in the transaction that is made within the economic or professional activity, or as part of any job function, or a person who uses an official service, a client or the factual beneficiary is a politically exposed person, a member of the family of the politically exposed person or a person who is considered to be a close employee of the politically exposed person, and the obliged person takes inspection measures as follow:
1) obtaines the approval from the higher management to create or maintain business relations with this person;
2) takes measures to identify the origin the wealth of that person and sources of those monetary funds that are used for business relations or when making occasional deals;
3) monitors those business relations on enhanced basis.
4.2.6. The authorized person should perform ongoing daily monitoring of politically exposed persons.

V. Scope and procedure of verification obligation

5.1 The Service provider takes verification measures both when building client relations, and during the validity of such relations, in respect of both individuals and legal entities, in accordance with the current legislation. The content and scope of verification measures depends on the degree of risk of the client and other factors of client relations.

[2] Different databases, such as Worldcheck and others that contain data to identify politically exposed persons.
[3] Public databases also refer to databases containing data on politicians and government members available on the Internet.

5.2 The procedure of verification measures as described in chapters III and V of this instruction shall be applied by the Service provider to each client whose transaction value is over 15 000 Euro or the equivalent amount in another currency (occasional transaction).
5.2.1. Identification of the client or person participating in occasional transactions and verification of information provided based on data obtained from the reliable and independent source, including via electronic identification and means to verify electronic transactions;
5.2.2. Identification of the representative of the client or person participating in occasional transaction, as well as identification and verification of right of representation of thereof;
5.2.3. Determination of beneficiary de facto and taking measures to verify identification thereof to the extent that allows the obliged person to ensure that the former is aware to be the de facto beneficiary and understands the ownership and control structure of the client or person participating in occasional transaction;
5.2.4. Understanding of business relationships, occasional deal or transaction, and, if appropriate, collection of more information about them;
5.2.5. Obtaining information on whether a person is a politically exposed person, his family member or a person considered to be his close associate;
5.2.6. Monitoring of business relations that should include at least the following:
5.2.6.1. Transaction is controlled during business relations to ensure compliance of transactions.
5.2.6.2. regular update of relevant documents, data or information compiled during verification measures;
5.2.6.3. Determination of the source and origin of means used for the transaction;
5.2.6.4. Paying greater attention during the economic, professional or official activities to transactions made within business relations, to client actions and circumstances indicating a criminal activity, money laundering or terrorist financing, or whose connection with money laundering or terrorist financing is obvious, including complicated, expensive and unusual transactions and patterns of transactions with no reasonable or obvious or legitimate purpose, or that are not typical to the specifics of certain business type;
5.2.6.5. Paying greater attention, during the economic, professional or official activities, to business relations or transactions if the client is from a third country posed at a greater risk or from a country/territory specified in AML/CTF legislation, or if they are citizens of that country, or if the place of residence or location of that person or location of the payment service provider is at a third country/territory posed at higher risk.
5.3. Enhanced verification measures shall be applied to customers with higher risk and in cases otherwise referred to in this instruction.
5.4. Verification measures should be intensified if:
- In the identity or information verification is suspected in terms of authenticity of data submitted or of documents, or identification of the actual beneficiary or actual beneficiaries is suspected;
- identity is verified of the person who is involved in the transaction to be made, or of the client, and the information submitted is verified when maintained in the place same as the place for that person or client;
- a person involved in a deal committed as part of business or professional activity, or during official operations, shall be the PEP of another Member State of the EEA or a third country, a family member or a close employee of such person;
- a person who participates in a transaction performed as part of economic or professional activity or an official function, or a person using an official service or a client is from a third country of a higher risk, or if their residence or business place or location of the payee's payment service provider are in a third country of a higher risk;
- a client or person party to a transaction, or the person using the official service, is an immigrant of that country or territory, or their place of residence or business place or location of the payee's payment service provider is in that country or in that territory where, as per such reliable sources as mutual evaluations, reports or published follow-up reports, there are no effective anti-money laundering and terrorist financing systems that comply with recommendations of the Financial Action Task Force (FATF), or that are considered to be in a low tax rate territory;

- the nature of the case is associated with higher risk of money laundering or terrorism financing;
- if the established risk analysis reports that in case of a given economic or professional activity or a given field of activity or given circumstances, it is a case posed at a risk of money laundering or terrorist financing exceeding the permissible risk.

5.5. For high-risk customers, the Service provider shall use at least one of the following enhanced verification measures:

- person Identification and verification of information submitted based on additional documents, data or information obtained from reliable and independent sources, or from any credit institution or a branch of a foreign credit institution, entered from a credit institution registered or having a place of business in a Member State of the EEA Agreement or in a country where similar requirements for anti-money laundering apply, and if a person is identified in this credit institution at the same place with the identifiable person;
- integration of any additional measures to ensure authenticity of documents submitted and correctness of data contained therein, in particular, the requirement of their certification by notary or official authority, or correctness of the data issued by the credit institution referred to in sub-clause 1;

VI. Application of verification measures as intensified

6.1. The obligated person takes verification measures on intensified basis to timely manage the risk of money laundering and terrorist financing that exceeds the usual risk and minimize it. Verification measures should be intensified if:

6.1.1. Identification of a person or client involved in the transaction and verification of data shall be performed without staying in the same place with the person or client to be identified;

6.1.2. In the identity or information verification is suspected in terms of authenticity of data submitted or of documents, or identification of the actual beneficiary or actual beneficiaries is suspected;

6.1.3. A person involved in a deal committed as part of business or professional activity, or during official operations, or a person using an official service, or a client, is the PEP (except the local politically exposed person), their family member or a close employee;

6.1.4. A person who participates in a transaction as part of economic or professional activities or an official function, or a person using an official service, or a client, is from a third country of a higher risk, or their place of residence or business location or location of the payee's payment service provider is in a third country of a higher risk;

6.1.5. A client, or a person participating in the transaction, or a person using the official service, is from such country or territory, or their place of residence or business location or location of the payee's payment service provider is in such country or in such territory where, as per such reliable sources as mutual evaluations, reports or published follow-up reports, there are no effective anti-money laundering and terrorist financing systems that comply with recommendations of the Financial Action Task Force (FATF), or that are considered to be in a low tax rate territory.

6.1.6. The nature of the case is associated with higher risk of money laundering or terrorism financing.

6.1. 7. The obligated person takes verification measures on the intensified basis even if the risk analysis prepared as per provisions of the AML/CTF states that, in case of a given economic or professional activity or a given field of activity or such circumstances, it is the situation with the risk of money laundering or terrorist financing exceeding the permissible risk. When assessing specific risks associated with the certain client, the obliged person, as per the AML/CTF, determines the risk profile of the client or the person participating in the transaction, taking into account the risk assessment, and at least the following circumstances:

1) information collected by the obliged person;
2) the scope of property maintained by the client, or the property scope of the transaction or transactions made during the official operation;

3) anticipated duration of business relations.
6.2. In cases above, the company's employees should apply at least one of the following intensified verification measures:
6.2.1. Person identification and verification of the submitted information on the basis of additional documents, data or information obtained from reliable and independent sources or from a credit institution or a branch of a foreign credit institution, Entered in the commercial register from a credit institution registered or having a place of business in a Member State of the EEA Agreement or in a country where the requirements equivalent to the provisions of the AML/CFT are in force, and if a person is identified at the same place with the identifiable person in this credit institution;
6.2.2. Integration of any additional measures to ensure authenticity of documents submitted and correctness of data contained therein, in particular, the requirement of their certification by notary or official authority, or correctness of the data issued by the credit institution referred to in sub-clause
6.2.3. First payment effected in relation to the deal via the account opened on behalf of the person or client involved in transaction with the credit institution registered or whose place of business is in the territory of a state-member to the agreement on European economic space or in a country where requirements apply that are equivalent to those of AML/CFT.

VII. Refusal to conclude an agreement and make a transaction

7.1. The company does not conclude agreements and does not make transactions:
7.1.1. With a person under 18 years of age;
7.1.2. With a person who refuses to submit information and documents specified in Section III of this instruction, or submits less data than required, or makes attempts to conceal something;
7.1.3. With a person suspected of being a false person;
7.1.4. With a legal entity of complicated and incomprehensible structure, and the actual beneficiary that is impossible to identify.
7.1.5. With a person who, based on documents submitted and/or based on information received by the company's employees, is suspected to be involved in money laundering or financing of terrorism;
7.1.6. With a person against whom international financial sanctions are in force. This information should be verified by employees on the website of the Anti-Money Laundering Compliance Unit.

VIII. Approach based on risk assessment and determination of client risk level

8.1. The taking measures to counteract money laundering and terrorism financing, the risk assessment approach should be considered. When creating business relationships, all verification measures should be applied, though the scope and accuracy of procedures depend on the type of customer and nature of business relationships and services.
8.2. The Service provider performs all verification measures. The scope of measures depends on the nature of specific business relationship or service, or on the risk level of the person or client involved in the deal, including the case when the principle "Know Your Client" applies.
8.3. When assessing the risk of money laundering and terrorist financing, the Service provider shall consider three risk categories: geographical risk, customer risk and risk associated with service. 8.3.1. **Geographical risk** is considered to be high if the client is known to relate to the following countries or territories:
- countries and territories subject to sanctions, embargoes or other similar measures of the United Nations (hereinafter referred to as the "UN") or the European Union (hereinafter referred to as the "EU");

- countries that do not have sufficient anti-money laundering and terrorist financing measures applied as defined by the Financial Action Task Force (FATF)) or European Union;
- countries that, as per reliable data, are associated with those to support terrorism, or those where the level of corruption is high.

8.3.2. **Client's risk** is considered to be high if the client:
- is such a person or his relationships with other persons are so much confusing or unusual that the actual beneficiary is impossible to define;
- is the PEP;
- Included in the UN or EU list maintained against persons subject to international financial sanctions (published on the website of theAnti-Money Laundering Compliance Unit);
- is a person who is previously suspected to be likely related with money laundering or terrorism financing.
- The client's behavior, appearance and transaction value are suspicious. The following factors shall indicate the suspicious person:
- appearance of the person and his/her behavior are inconsistent with the nature of transaction performed by the person, or the conduct of the person is not trustworthy;
- the person seeks third party help to complete documents or fails to know how to fill them;
- the person's representative makes attempts to conceal the actual client or is not aware of client data;
- a person attempts to conclude a fictitious or other illegal transaction;
- a person is suspected to make a transaction on the name and the expense of person other than him;
- a person is known to be involved in money laundering.

8.3.3 **Risk associated with transaction** is considered to be high if:
- the value of transaction exceeds 15 000 Euro or the equivalent amount in another currency;
- a third party pays for transaction in cash who is not a party to the transaction.

8.3.4. The risk associated with communication or mediation channels between the obligated person and clients or with channels for product, service or transaction transfer.

8.4. When determining the degree of risk for the person, the client residence matters, as well as that of the actual beneficiary, and in case of non-resident client, the PEP status matters. The degree of risk shall be formed as follows:

Low degree:

1. a private person-resident that is the actual beneficiary;
2. an official-resident and non-resident (for example, bailiff, notary).

Moderate degree:

1. a private person-non-resident that is the actual beneficiary of the service and is not PEP;
2. a private person-resident that is not the actual beneficiary of the service.

High degree:

1. a private person-non-resident that is PEP;
2. a private person-resident that is not the actual beneficiary of the service;
3. a private person-non-resident coming from the FATF monitoring country[4].

8.5 **The risk of money laundering or terrorist financing shall be considered high whenever, for any reason, there is suspicion that the client or the client's transaction may be related to money laundering or terrorist financing.**

8.6 If at least one risk factor applies to the client or transaction as specified in clause 8.3, the client shall be subject to intensified verification measures.

8.7 If relationships are built with the client subject to intensified verification measures, an employee shall immediately inform the contact person of the Service provider by email or telephone.

IX. Instructions to define transactions suspected in money laundering

[4] FATF monitoring countries - Albania, The Bahamas, Barbados, Botswana, Cambodia, Ghana, Jamaica, Mauritius, Myanmar, Nicaragua, Pakistan, Panama, Syria, Uganda, Yemen, Zimbabwe.

The purpose of this instruction is to help the authorized persons to identify suspicious deals indicating money laundering. If the term "person" is not specified in the list of suspicious transaction signs (hereinafter referred to as "the list"), then both the natural person and the legal entity shall apply to the term. In terms of suspicion of money laundering and financing of terrorism, suspicious transactions shall be transactions and client operations that miss any clear economic or legal reason and that cannot be considered as regular economic activity of the client.

9.1. Below find factors that indicate suspicious transactions in the case of transactions with virtual currency exchange services for money that exceeds 15 000 Euro or the equivalent amount in another currency:

9.1.1. a person cannot be identified or makes attempt to avoid submission of his/her identification data;

9.1.2. the person's representative makes attempts to conceal the actual transaction party or is not aware of personal data of the former;

9.1.3. a person attempts to conclude a fictitious or other illegal transaction;

9.1.4. a person is suspected to make a deal on behalf of other person;

9.1.5. a person is known to be involved in money laundering;

9.1.6. a person intends to make payments for the amount of over 15 000 Euro or for the equivalent amount in another currency;

9.1.7. a person repeatedly makes payment for the sum over 15 000 Euro or on the equivalent sum in other currency;

9.1.8. a person makes a payment that is a bit smaller than the maximum amount that requires person identity (15 000 Euro or the equivalent amount in other currency);

9.1.9. a payment is made via a front company or by the bank transfer located on a tax-free territory;

9.1.10. a payment is preceded by the payment of the amount over 15 000 Euro or equivalent amount in another currency to the third person's account.

9.2. Suspicions when concluding a client agreement

9.2.1. An individual is suspected to be false:

9.2.2. appearance of the person and his/her behavior are inconsistent with the nature of transaction performed by the person, or the conduct of the person is not trustworthy;

9.2.3. the person seeks third party help to complete documents or fails to know how to fill them;

9.2.4. a person is not aware of the nature of activity of legal entity represented by him;

9.2.5. a person is not aware of actual beneficiaries (owners) of the legal entity represented by him or location or contact details of the latter;

9.2.6. a person fails to describe his/her potential partners and/or the scope of the latter;

9.3. A legal entity is suspected to be false:

9.3.1. representatives of a legal entity cannot be uniquely identified in the documents (no personal code or date of birth);

9.3.2. a legal person is registered in the region where sufficient measures of identification of persons and other measures of counteraction to money laundering are not applied;

9.3.3. mailbox is specified as the address of the legal entity;

9.3.4. the residence address is specified as the legal address of a legal entity and this is not consistent with the alleged/approved scope of activity;

9.3.5. a legal entity has no contact telephone number;

9.3.6. a legal person is known to the bank of previous suspicion to act as a false person

9.4. Unusual documents:

9.4.1. the power of attorney of the person or his identity documents do not meet requirements by form;

9.4.2. the power of attorney of the person or his identity documents that are are invalid;

9.4.3. The documents submitted are suspected to be falsified.

9.5. When concluding client contracts:

9.5.1. a person fails to justify the need in service for purpose of which they apply to the Trader;

9.5.2 a person wishes to specify a person as the user of property leased, who is not related with him by activity or personally.
9.6. When making transactions:
9.6.1 Unusual deal with money:
9.6.1.1 individual large (over 15 000 Euro or equivalent amount in other currency) or regular cash payments, even for smaller sums, if they do not comply with economic activity of the person or his usual turnover;
9.6.1.2 there are other signs unmentioned that may indicate the illegal activity.

X. How to identify and manage risks associated with technologies

Terms

Information System is the technical system that processes, records or transmits data all along with the means required for its normal operation, resources and processes.
Risk Analysis for Information System is the analysis that requires identification of potential hazards and weaknesses of the critical information system, probability of implementation of hazards and the associated damage will be assessed, as well as the choice of suitable safety measures to reduce the impact of hazards.
Information Asset - information, data and applications and technical means required for their processing.
Confidentiality is the availability of information asset for authorized consumers only (persons or technical systems) and inaccessibility for others.
Availability is timely and convenient availability and applicability of data for authorized consumers. Timely and uncomplicated availability of information assets applicable for use for the predetermined required/specified working time (i.e., at the required/needed time and during the required/need period) for consumers authorized to do so (persons or technical systems).
Vulnerability is the weak point of information asset that may be used for one or more dangers to appear.
Danger is an event or circumstance that may cause interruptions in availability or otherwise damage the information asset.
Risk is the assessment that considers uncertainty for circumstances that may interfere with the ability of an institution or enterprise to deliver a vital service within a time frame of quality or planned scope. The risk for information security is often expressed as a combination of event consequences in the field of information security and likelihood of the event. Identification of technological risks Risk is identified by the risk analysis. Probabilities and consequences shall be assessed based on the qualitative risk analysis method.
The qualitative risk analysis should always rely on the analysis of different risk scenarios, taking into account the importance of hazards and the cost of protected assets, as well as their potential weak points. It is necessary to rely on the previous experience and knowledge of appraisers to give the assessment and conclusion. In case of qualitative analysis of risks to evaluate potential consequences and rate of occurrence of incidents, step-by-step classifications are used based on scales. The step-by-step scale for qualitative analysis of risks of expenses of definitions shall be given as interpreted by the Department of State Information Systems.
10.1. Technology Risk Management
Risk management is the process to manage methods to handle risks identified, as well as to implement a risk mitigation method in line with tolerance to risk.
The risk is reduced, in particular, through audits. This measure may be taken to reduce one or more specific risks or weak points. Continuous monitoring and review of risks
- the verification is mandatory in case of occurrence of each dangerous situation.

10.2. As per these procedural rules, an enterprise that uses the latest IT-technologies should take it risks seriously. To arrange internal and external processes, it is recommended to follow a range of requirements by standards ISO/IEC 27000 and NIST (if possible).
10.3. Important points:
• The first internal audit of ISO 27002 standard should be completed within two weeks your clients and employees should be checked through public databases;
• It is necessary to mark and classify the information that goes through the company.
• all drives are encrypted. The company should practice safe destruction of media at the end of their service life;
• It is necessary to keep track of accounts, especially administered accounts Last Pass and Apple keychain should be used to record important information, such as passwords;
• Data should be backed up every day; monthly testing of backup copies is required;
• Information security should be ensured. Secure development policy and responsibility for asset control.

XI. Reporting to the Anti-Money Laundering Compliance Unit and actions when money laundering is suspected

11.1. If the Service provider, in the course of its business activity, reveals an action or circumstance hat is suspected to be the money laundering, terrorism financing or an attempt to do so, or in terms of which the Service provider suspects or knows that it was involved in money laundering or terrorism financing, he shall be obliged to immediately, but not later than within **two business days** since the date of action or circumstance identification, or since the moment of suspicion, notify the **Anti-Money Laundering Compliance Unit**.
11.2. The employee should inform the contact person and AMLCU of each transaction with the financial obligation of over 32 000 Euro or the equivalent amount in another currency made in cash, regardless of whether the transaction is made in the form of one payment or in the form several payments related to each other. The mention notification duty shall arise based on the amount and does not depend on whether the employee suspects the case of money laundering or not.
11.3. The Service provider, its business partner, member of the governing body and employee of the Service provider and its business partner shall be prohibited to inform the person or actual beneficiary of that person of the message communicated to the Anti-Money Laundering Compliance Unit, as well as the initiation of criminal case under AML/CFT.
11.4. The communication shall be transmitted orally, in writing or in a form that allows written reproduction. If the message is communicated orally, it shall be repeated no later than the next business day in writing or in format that allows written reproduction. Data used to identify the person and to verify the information submitted, and, if necessary, copies of documents may be attached to the message.
11.5. **Information shall be communicated to the Anti-Money Laundering Compliance Unit: at the postal address: Aadress: Pärnu mnt 139, 15060 Tallinn Klienditugi (E-R 9.00-17.00): 612 3000 Faks: 612 3009 E-post: ppa@politsei.ee Töötajate e-posti aadressid: eesnimi.perekonnanimi@politsei.ee**

XII. Data Registration and Storage

12.1. The Service provider shall keep copies/electronic copies (e-storage) of documents that serve as the ground to identify the person and verification of information submitted, as well as information obtained during the creation of business relationship, at least for five years upon termination of business relations.
12.2. The Service provider shall keep the data for at least five years upon transaction in a way that allows their retrieving, if necessary.
12.3. The Service provider shall keep all messages in the form that allows written reproduction, received from employees on suspicious and unusual transactions, as well as information collected to

review such messages and other related documents, as well as messages communicated to Anti-Money Laundering Compliance Unit, along with data on terms of data submission and employee for 5 years.

12.4. The Service provider shall allow regular updates and relevance of client information (including documents and data collected), and ensures that the aforementioned information is updated and is relevant by updating data each time when it delivers service to the client based on the transaction of single service.

12.5. The Service provider shall keep the information and documents relating to person identity in a manner that allows response, in full and without undue delay, to relevant inquiries from the Anti-Money Laundering Compliance Unit, the investigating authority, the court or the supervisory authority.

XIII. Delegating an activity

13.1. The delegation (assignment) of activities, as specified by these procedural rules, mainly verification measures (e.g. person identification), to a third party may arise due to the need in more effective performance of duties related to their own economic activities. When delegating activities to a third party, the Service provider shall bear full responsibility for violation of requirements.

13.2. When delegating activities, the Service provider enters into a written contract with a business partner. An activity may be delegated only if:

1. this shall not harm the legitimate interests of the Service provider;
2. this shall not preclude the activities of the Service provider, as well as the obligation to resist money-laundering and terrorism financing;
3. this does not preclude the state supervision over activities of the Service provider;
4. a third party, to whom the activity is delegated, has the required knowledge and skills and is capable of meet all requirements related to anti-money laundering and terrorism financing;
5. The Service provider shall be entitled to control compliance with requirements by a third party related to counteraction of money laundering and terrorism financing;
6. the provision is ensured that documents and data collected to meet requirements of anti-money laundering and terrorist financing shall be kept as per the established procedure;

13.3. The Service provider undertakes to inform the management of his business partners of requirements related to anti-money laundering and terrorism financing and to ensure training to their employees in the area of anti-money laundering and terrorism financing. Moreover, the Service provider undertakes to inform his partners' personnel, upon the training, at least once a year of the nature of risks of money laundering and terrorism financing, as well as of new trends in this area. First of all, the personnel should be informed of requirements governing anti-money laundering and terrorism financing, application of verification measures, recognition of suspicions of money laundering and related reporting.

13.4. The Service provider shall immediately report on authority assignment to the Anti-Money Laundering Compliance Unit.

XIV. Employee Training

14.1. The contact person shall take measures, on a regular basis and as necessary, to hold trainings to clarify requirements and obligations set out in regulations, providing, inter alia, the information on modern methods of money-laundering and terrorism financing, and risks involved.

14.2. Primary education in money laundering shall be held during personnel recruitment and employees directly engaged in customer service shall be trained once a year.

14.3. When holding trainings, the contact person shall rely on following circumstances:
- an opportunity coming from the position of the employee that allows the chance to deal with unusual transactions that may be related to money laundering and terrorism financing;
- typical cases of suspicious and unusual transactions that may occur in the sphere of activity of the employee, and preventive measures applied;
- application of sanctions in terms of workers who fail to comply with requirements of law or legal acts approved on its basis to counteract money laundering and terrorism financing.
14.4. The contact person shall keep records of trained employees specifying the training discipline, its duration, name and surname of the person involved in it.

XV. Internal Control Operations

15.1. The system of internal control of the Service provider is based on that the direct supervision of compliance with rules by employees is made by the management.
15.2. By the check result, the Board/Managing Partner shall make the verification report containing at least the following information: purpose of check; time of check; name, surname and title of the controller; description of check performed; analysis of check results or general check conclusion.
15.3. If the check reveals flaws in using rules, the controller adds descriptions of deficiencies to the report, along with the description of associated potential risks. The check reveals the period required to correct deficiencies, defects, recommended measures used to correct defects, shortcomings, and the period for verification upon defect elimination. During the check and upon verification of deficiencies, the report shall be accompanied with the analysis of results of checking upon elimination of defects, as well as the list of remedial measures indicating the time actually spent for remedies.
15.4. Due to verification of compliance with anti-money laundering and terrorism financing activity, the Board/Managing Partner has the following responsibilities:
1. to verify compliance with measures to resist money laundering and terrorism financing;
2. to assess the need for employee training;
3. to analyze the results of the compliance test.
15.5. Due to verification of compliance with anti-money laundering and terrorism financing activities, the Board/Managing Partner has the following rights:
1. To monitor the performance of personnel and obtain technical means required for that;
2. To require immediate termination of requirement violation in the field of counteraction to money laundering and terrorism financing;
3. To make suggestions on elimination of deficiencies found during the check, including those relating to modification and supplementing procedural rules.
15.6. The Service provider performs the internal check at least once a year.

XVI. Contact person

16.1. The contact person shall be appointed by the decision of the Board/Managing Partner of the Service provider.
The Board/Managing Partner of the Service provider shall be involved in duties of the contact person until it is assigned.
16.2. The tasks of the contact person shall include:
- arrangement of procedure to collect the data indicating unusual transactions or transactions suspected of money laundering or terrorist financing revealed in terms of activities of the Service provider and its analysis;
- instruction, training and awareness among employees on the procedure to counteract money laundering and terrorism financing;
- verification of compliance with requirements to counteract money laundering;
- regular written reviews of compliance with procedural rules, as well as informing employees of shortcomings and actions to eliminate the latter;

- monitoring of client's transactions and their control;
- communication of information to Anti-Money Laundering Compliance Unit in case of suspicion of money laundering or terrorism financing;
- responses to inquiries submitted by the terrorism and enforcement of its regulations;
- arrangement of actions to enforce decisions and notifications containing international sanctions.

16.3. Contact person's rights:
- to check compliance of execution of transactions and operations with legal acts and rules;
- to check actions of employees and implementation of measures against money laundering or terrorism financing, as well as to requires immediate cessation of violation of requirements in the field of counteraction to money laundering and terrorism financing;
- to modify and supplement rules to counteract money laundering and terrorism financing;

16.4. The contact person shall be given the access to information that serves the ground or prerequisite to create business relations, including the information, data and documents to prove the client's identity and economic activity thereof.

16.5. The contact person may communicate the information and data that has become known to him in connection with suspicion of money laundering and terrorism financing and/or with application of international sanctions vested to this employee, Anti-Money Laundering Compliance Unit, agency of inquiry (preliminary investigation) in connection with criminal proceedings or the court based on the court order or decision.

16.6. The Service provider shall notify the Anti-Money Laundering Compliance Unit within the reasonable period of time of the contact person appointment or change in contact details, communicating the relevant decision of the Board/Managing Partner to the Anti-Money Laundering Compliance Unit.

XVII. International Sanctions

17.1. International financial sanctions as per AML/CTF legislation shall be international sanctions that shall, completely or partially, prevent the subject of international, financial sanctions to use and dispose of cash means, and that these assets be transferred to be disposed of, including prohibiting or limiting:

1) provision of loans and credits to the subject of international financial sanctions or otherwise payment of assets to him based on similar nature;
2) payment to the subject of international financial sanctions of deposits, dividends, interest and other similar funds in cash, promissory notes, cheques or other means of payment and payment means, as well as alienation, pledge and transfer to use and dispose of securities, precious metals and stones or other such values;
3) opening of the deposit or settlement account, securities account or other account for the subject of international financial sanctions, granting to use the safe or conclusion of contracts on rendering such services;
4) making deals with the subject of international financial sanctions with real estate, fixed by the courts, movable things or rights entered with the register;
5) a pledge of monetary funds and economic resources to the subject of international financial sanctions or otherwise provision thereof as collateral;
6) conclusion of the insurance contract with the subject of international financial sanctions and making payments based on such contract;
7) Establishment or continuation of business relations with the subject of international financial sanctions.

- The foregoing applies also if the subject belongs to several persons as the shared or joint property, where at least one of them is subject to international financial sanctions.

- The subject of international financial sanctions may be:

1) a state, territory, territorial unit, regime, organization, association or formation in respect of which measures are taken as specified by a legal act to set forth international financial sanctions;
2) a natural person or legal entity, institution, partnership or any other unit that is directly mentioned in the legal act specifying international sanctions, and in respect of which measures are taken under the legal act setting forth international sanctions.
17.2. When creating business relations and throughout all business relations, special attention should be paid to activities of the person and circumstances indicating the likelihood that the person is the subject of international financial sanctions, as well as immediately notify the contact person of identification of the subject of international financial sanctions, of suspicion and measures taken.
17.3. If the employee suspects that the client is the subject of international sanctions, the client should be required to submit additional information that will be helpful to identify the status of that person. If such a person refuses to submit additional information or it is impossible to identify whether a person is the subject of international sanctions, business relations shall not be build with the person or deal shall not be made with the client; measures shall be taken as required by international sanctions and the Anti-Money Laundering Compliance Unit should be informed.
17.4. Subjects of International Sanctions shall be checked by the Service provider at the page of the website Anti-Money Laundering Compliance Unit, typing the name and surname of the person to verify. The Service provider undertakes to make sure that the person involved in the transaction is not subject to international sanctions when creating business relations, during cooperation and when delivering services to the person. Persons shall be verified as per the sanction list manually, and the following data shall be kept for 5 years: check time; name of controller; check results; measures taken.
17.5. The contact person shall immediately notify the Anti-Money Laundering Compliance Unit if reveals that the person who intends to create business relationship with the Service provider or that has already concluded business relations shall be the subject to international sanctions, or if the person is suspected to be the subject of international sanctions. The access to services shall be immediately ceased for the client and international sanctions shall be applied in view of their content and volume.
17.6. The authorized person should perform ongoing daily monitoring of international sanctions and to check the subjects of international sanctions.

XVIII. Risk management for the concern

18.1. If an obligated person entering the concern as a parent company applies internal procedural rules of the concern and by-laws to control their compliance, regardless of whether all enterprises belonging to the concern are located in the same country or in different countries. This obligation includes, in particular, introduction of the by-law to share information regarding money laundering and terrorism financing, as well as introduction of rules to protect similar personal data. The obligated person ensures that internal procedural rules of the concern and by-laws duly consider the right of another member state of the European Union to which the Directive No. 2015/849of the European Parliament and Council (EC) applies, if the obligated person has a representation, branch or subsidiary with majority ownership in that state -member of the EU.
18.2. If the obligated person has a representative office, branch or subsidiary with a majority share in a third country where the minimum requirements for anti-money laundering and terrorism financing are not equivalent to requirements of the Directive No 2015/849 of the European Parliament and Council (EC), such representative office, branch or a subsidiary with a majority share apply procedural rules and by-laws that comply with requirements of this law, including requirements for protection of personal data to the extent that is permitted by law of a third country.
18.3. If the obligated person reveals circumstances where procedural rules and by-laws are not feasible to apply in their representative office, branch or subsidiary with majority share pursuant to the

right of a third country, that comply with requirements of this law, they shall notify the relevant supervisory authority thereof. The relevant supervisory authority shall notify supervisory authorities of the Member States of the EU and, if appropriate, supervisory authorities of the European Union if, pursuant to the first sentence of this part, it is revealed that a third country is not eligible to apply procedural rules and by-laws in the concern that comply with requirements of the Directive No. 2015/849 of the European Parliament and Council (EC).

18.4. In the case specified in clause 18.3 of this chapter, the obliged person ensures that additional measures are taken at the representation office, branch or subsidiary with the majority share that shall be applied otherwise to efficiently manage risks related to money laundering or financing of terrorism, having informed the supervisory authority of measures taken. In such a case, the relevant supervisory authority shall be entitled, via its decision, in particular, to require the following from the obliged person and the representative office, branch or subsidiary with the majority share of the obligated person:

1) not to create new business relations in this country;
2) to cease business relations maintained in this country;
3) to suspend service provision, in full or in part;
4) to cease their activity;
5) to apply other measures as prescribed by the regulatory technical standards as specified by the European Committee based on Part 7 of Article 45 of the Directive No. 2015/849 of the European Parliament and Council (EC).

18.5. Within the concern, the information on suspected cases reported to Anti-Money Laundering Compliance Unit may be shared, unless the Anti-Money Laundering Compliance Unit prescribes otherwise.