AML Policy

Last updated: May 24, 2021

I. GENERAL PROVISIONS

1. These Rules for The Prevention of Money Laundering and (or) Terrorist Financing (hereinafter – the **Rules**) are prepared to ensure the prevention of money laundering and terrorist financing in activity of VienPay UAB (hereinafter – the **Company**).
2. The Rules describe how the Company will organize and ensure the adequate anti-money laundering and counter terrorism financing procedures. The implementation of the Rules will ensure that the name, reputation and financial integrity of the Company, whilst ensuring compliance with all necessary laws and regulations.
3. The provisions of the Rules must be adhered to by all operations, organisation and staff of the Company.
4. The Rules are prepared in accordance with the Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania (hereinafter – the **Law**) and other applicable legal acts of the Republic of Lithuania.
5. Unless the Rules state otherwise, all terms used therein have the meaning indicated in the Law and other applicable legal acts.

II. DEFINITIONS

1. Unless otherwise required by the context, the following terms beginning in a capital letter shall be taken to have the following definitions:

    1.1. **Customer** – a legal or natural person performing monetary operations or concluding transactions with the Company;

    1.2. **Company** – VienPay UAB, legal entity code 305744365, registered address at Nagevičiaus g. 3, Vilnius, Republic of Lithuania;

    1.3. **Responsible Employee** – an employee appointed by the CEO who is responsible for the implementation of measures for the prevention of money laundering and (or) terrorist financing in accordance with the Rules;

    1.4. **Prominent Public Functions –** functions which are listed in Article 19(2) of the Law or are included on the list of prominent public functions published by the FCIS;

    1.5. Close Family Member – spouse, a person with whom a civil partnership is registered, parents, siblings, children and spouses or civil partners of children;

    1.6. Business relationship – a business, professional or commercial relationship between a Customer and the Company which is connected with their professional activities and which is expected, at the time when the contact is established, to have an element of duration.

1.7. Beneficial Owner – a natural person, who is the owner of a Customer (a legal person) or controls the Customer, and/or a natural person for the benefit of which a transaction or activity is being conducted. The Beneficial Owner is considered to be**:**

a) In a legal person:

(i) a natural person who owns the legal person or who controls it either directly or indirectly by owning a sufficient percentage of the legal person's shares or voting rights, including bearer shares and control through other means, other than a company listed on a regulated market that is subject to disclosure requirements consistent with EU law or subject to equivalent international standards which ensure adequate transparency of ownership information;

(ii) a natural person holding 25 % plus one share or an ownership interest of more than 25% in the legal person is considered to be a direct owner. A natural person holding 25 % plus one share or an ownership interest of more than 25 % in a legal entity or entities which control or hold 25 % plus one share or an ownership interest of more than 25 % in a legal entity is considered to be an indirect owner;

(iii) a natural person performing the role of the senior manager if the person in point (i) above cannot be determined or there are doubts on whether the person determined is the Beneficial Owner;

b) in the case of trusts:

(i) the settlor;

(ii) the trustee(s);

(iii) the protector, if any

(iv) the beneficiaries, or where the individuals benefiting from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates;

(v) any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means;

c) in the case of legal entities such as foundations, and legal arrangements similar to trusts, the natural person(s) holding equivalent or similar positions to those referred to in point (b);

1.8. **EU Member State –** a member state of the European Union or the European Economic Area;

1.9. **Third Country –** a country which is not a member state of the European Union or the European Economic Area;

1.10. **FCIS –** The Financial Crime Investigation Services under the Ministry of the Interior of the Republic of Lithuania;

1.11. **Politically Exposed Person (PEP) –** a natural person who is carrying out or has carried out Prominent Public Functions, their Close Family Members and Close Associates. A person who has not carried out Prominent Public Functions during at least the last year by the date of entering the Business relationship or making of a transaction or such a person's Close Family Members or Close Associate are not considered as politically exposed persons;

1.12. **Suspicious Financial Operation –** a monetary transaction, which is performed with funds, which are suspected to have been received (either directly or indirectly) from criminal activities or from participating in such activities or/and are related to terrorist financing;

1.13. **Close Associates –** natural persons who are known to have joint Beneficial Ownership of legal entities or legal arrangements, or any other close business relations, with a Politically exposed person and (or) natural persons who have sole Beneficial Ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a Politically exposed person**;**

1.14. **Virtual Currency** – an instrument with a digital value but no legal currency or monetary status, which is not authorized or guaranteed by a central bank or other public authority and which is not necessarily pegged to currency but which is recognized by natural or legal persons as an exchange instrument and which is transferable and sold electronically;

1.15. **Virtual Wallet** – public key addresses which are generated for virtual currency addresses for the storage and management of virtual currencies entrusted to other natural or legal persons (third parties) but remaining in their ownership.

III. CUSTOMER IDENTIFICATION

1. The Company takes all necessary, proportionate measures in order to identify its Customer and to verify the identity of the Customer and Customer's Beneficial Owners. The Company takes measures and determine identity of the Customer or his representative in the following cases:
   1.1. before establishing a Business relationship;
   1.2. before conducting one or several related Virtual Currency transactions (exchanges) or allowing a deposit of Virtual Currency on a Virtual Wallet the value of which is equal to or exceeds EUR 1,000 at the time of the transaction and/or deposit;
   1.3. if there is suspicion that information previously provided about the Customer or his representative is incorrect and/or incomplete;
   1.4. in any other case, when there are suspicions that an act of money laundering and / or terrorist financing is, was or will be carried out.
2. The Company establishes Customer's identity only remotely, i. e. when the Customer is not physically present.

Remote Customer identification

3. The Company establishes Customer's (natural person's or legal person representative's) identity remotely by using the following measures:
   3.1. when using information from third parties about the Customer or the beneficial owner in accordance with the procedure laid down in the Law;
   3.2. when information about the Customer's identity is confirmed with a qualified electronic signature supported by a qualified certificate for electronic signature which conforms to the requirements of Regulation (EU) No 910/2014;
   3.3. when using electronic means allowing direct video streaming in one of the following ways:
      a) the original of the identity document or an equivalent residence permit in the Republic of Lithuania is recorded at the time of direct video streaming and the identity of the Customer is validated using at least an advanced electronic signature which conforms to the requirements laid down in Regulation (EU) No 910/2014;
      b) the facial image of the Customer and the original of the identity document or an equivalent residence permit in the Republic of Lithuania shown by the Customer is recorded at the time of direct video streaming.
4. In every case establishing Customer's identity remotely by using measures specified in paragraph 9 is allowed only when there are all conditions laid down in the Law.
5. When establishing Customer's identity remotely, the Company shall:
   5.1. verify whether there are any circumstances to apply enhanced Customer due diligence. If such circumstances are present the procedures for enhanced Customer due diligence accordingly shall be followed;
   5.2. assess whether the Customer provides copies of valid identity documents or corresponding travel documents which photographs are matching. This requirement does not apply if the identity is being determined using a qualified electronic signature;
   5.3. find out whether the Customer will act on his own behalf or someone else's interests;
   5.4. verify whether a representative has legal permit or power of attorney to act in the name of the Customer;
   5.5. to receive additional documents with the necessary information, if additional information is required from the Customer;
   5.6. check whether Customer or Customer's beneficiary is included in the list of people that are financially sanctioned by Lithuania, European Union (EU sanctioned person list) and United Nations;

5.7. use reliable and independent sources to verify whether the Customer is a PEP.

6. If the Customer is represented by another person, the Company shall request proof of power of attorney and, if possible, check its validity (i.e. if the Customer or its representative has the right to issue such a power of attorney), expiry date, actions that representative can undertake in the name of the Customer. Power of attorney shall comply with rules established in the Civil Code of the Republic of Lithuania. In case the power of attorney is given by the Customer natural person, such power of attorney on behalf of the Customer shall be certified by the notary.

IV. ESTABLISHING BENEFICIAL OWNER'S IDENTITY

1. The Company shall always establish the identity of Beneficial Owner of the Customer (in accordance to the Law and these Rules).
2. The Customer shall submit the following data on the Beneficial Owner:
   2.1. Name/names;
   2.2. Surname/surnames;
   2.3. Personal identification number (in the case of a foreigner: date of birth (where available – personal number or any other unique sequence of symbols granted to that person, intended for personal identification, the number and period of validity of the residence permit in the Republic of Lithuania and the place and date of its issuance);
   2.4. Citizenship.
3. The data submitted by the Customer shall be validated using electronic identification means issued in the European Union which operate under the electronic identification schemes with the assurance levels high or substantial, or with a qualified electronic signature supported by a qualified certificate for electronic signature which conforms to the requirements of Regulation (EU) No 910/2014, or using electronic means allowing direct video streaming.

V. PROHIBITION TO ENTER INTO A BUSINESS RELATIONSHIP

1. It is forbidden to start Business relationship if the Customer and / or his representative:
   1.1. fails to submit the data confirming his identity;
   1.2. submits not all the data or where the data are incorrect;
   1.3. avoids submitting the information required for establishing his identity,
   1.4. conceals the identity of the Beneficial Owner or avoids submitting the information required for establishing the identity of the Beneficial Owner or the submitted data are insufficient for that purpose;
   1.5. the Company, due to the Customer's actions or omissions, is not able to ensure proper compliance with the Law and the related legal acts.
2. In such cases, specified in paragraph 17, the Company shall, upon assessment of the threat posed by money laundering and/or terrorist financing, decide on the appropriateness of forwarding a report on a suspicious monetary operation or transaction to the Financial Crime Investigation Service of the Republic of Lithuania (hereinafter – the **FCIS**).
3. If the Company is unable to comply with points above, the Company shall not conduct business relations with such Customer. In these cases, the Responsible Employee of the Company has to evaluate possible money laundering or terrorist financing threat and inform the CEO and FCIS.
4. If the Customer avoids or declines a request by the Company to provide information on source of assets, money and etc., the Responsible Employee has to inform the CEO. In that case CEO shall make a decision to terminate Business relationship with the Customer and the Responsible Employee shall inform FCIS. The Responsible Employee has a responsibility to take immediate action to interrupt money laundering and / or terrorist financing.
5. Information gained identifying the Customer and beneficiary owner, monitoring Customer activities has to be documented either physically or electronically.

VI. CUSTOMER CLASSIFICATION FOR DUE DILIGENCE PURPOSES

1. All Customers should be classified according to the risks of being involved in money laundering or

terrorist financing (TF).

2. Risk categorization shall encompass three different Customers risk levels.
3. Such categorization shall be based on multiple parameters, including, but not limited to:
    3.1. Customer's identity;
    3.2. Customer's residency (registration place, if Customer is a legal entity);
    3.3. Nature of business activity;
    3.4. Actual location of business activities;
    3.5. Customer's (legal entity's) ownership and complexity of control structure;
    3.6. Nationality of Beneficial Owner;
    3.7. Volume and nature of transactions carried out by the Customer;
    3.8. Social / financial status;
4. The following Customer risk classification is used:
    4.1. **Low risk Customers**:
        a) In the cases specified by the European Supervisory Authorities and the European Commission.
        b) In the cases where the Customers are legal persons whose securities are admitted to trading on a regulated market in one or more EU Member States;
        c) In the cases where the Customers are entities of public administration – state and municipal institutions and institutions, the Bank of Lithuania;
        d) In the cases where the Customer is a financial institution covered by the Law (or a financial institution registered in another European Union Member State).
        e) The Customer is identified as low risk in accordance with the Company's Risk Assessment Procedure.

    4.2.**Medium risk Customers**:
        a) All other Customers not identified as low or high risk.

    4.3.**High risk Customers** – the Customer are categorized as high-risk Customer if one of the following criteria is applicable:
        a) The Customer or his / her representative or at least one of the Customer's Beneficial Owners is a PEP;
        b) During the identification procedure the Customer avoids performing actions necessary for the verification of his / her identity and providing information about him / herself;
        c) At the request of the Company, the Customer did not provide the documents evidencing the financial activities (documents evidencing the transactions concluded or being concluded by the Customer and other documents evidencing the financial activities performed or being performed by the Customer);
        d) The Responsible Employee of the Company establishes existence of the features unusual to the ordinary activities performed by the Customer (performance of monetary operations with larger amounts, complex transactions, transactions are carried out in an unusual pattern etc.);
        e) The Customer's age, official position, status and / or financial condition (low income of the Customer when compared with the extent of the Customer's financial activities) do not comply objectively with the financial activities performed by the said Customer;
        f) If a suspicion is raised during the monitoring of Customer's business relations with the Company.
        g) The Customer is determined to be of a high risk in accordance with the Company's Risk Assessment Procedure.

VII. INDENTIFICATION OF POLITICALLY EXPOSED PERSONS

1. The Company shall consider its Customers to be PEP's when at least one of the following criteria is met:
    1.1. A citizen on the Republic of Lithuania or the European Union declares that they have been entrusted with Prominent Public Functions or that they are Close Family Members or Close Associates of such a person (as defined in section I of the Rules);
    1.2. The Company's employees determine that the natural person is a PEP by using public sources and (or) by obtaining such information from third parties, such sources may include, but are not limited to the Chief Official Ethics Commission and commercial databases which list PEP's;
    1.3. A representative of a legal person declares that the shareholders (natural persons) of the legal person have been entrusted with Prominent Public Functions or that they are Close Family Members or Close Associates of such a person.

VIII. ENHANCED CUSTOMER IDENTIFICATION PROCEDURE

1. The enhanced Customer identification is performed:
    1.1. Where transactions or Business relationships are carried out with PEP's;
    1.2. In the cases indicated by the European supervisory authorities and the European Commission;
    1.3. If according to the risk assessment and management procedures established by the Company a higher risk of money laundering and / or terrorist financing is determined. When assessing the risks of money laundering and / or terrorist financing, it is necessary to assess the risk factors of possible increased money laundering and / or terrorist financing identified in these Rules.
2. When applying enhanced Customer identification procedure for Customers that are PEP's, the Company shall:
    2.1. Identify whether the Customer and (or) the Beneficial Owner of the Customer are PEP's;
    2.2. Get consent from the CEO of the Company to start or maintain Business relationship with that Customer, when he becomes a PEP;
    2.3. Take adequate measures in order to determine the source of assets and funds involved in Business relationship and contracts;
    2.4. Ensure identification of unusual transactions and regular review of the information about such Customer and its Transactions that the Company holds;
    2.5. Maintain enhanced activity monitoring of PEP's.
3. When a PEP stops holding important public positions, the Company shall, for at least 12 months, continue to consider the ongoing risks of that person and apply appropriate measures at the risk level, until it is determined that the person concerned no longer has the risk inherent in the Customer being considered a PEP.
4. When applying enhanced Customer identification procedure in the cases specified by the European Supervisory Authorities and the European Commission, the Company shall choose the measures referred to in the documents of the European Supervisory Authorities and the European Commission which identify such cases.
5. When applying enhanced Customer identification procedure if according to the Risk assessment procedure (Annex 1) a high risk of money laundering and / or terrorist financing is determined, the Company shall in all cases:
    5.1. Collect additional information on the Customer and / or its Beneficial Owner;
    5.2. Collect additional information about the nature of the Business relationship;
    5.3. Collect information about the purpose of the planned and / or executed Transactions;
6. Additionally, the Company in its discretion may apply any of the following measures in addition to the measures described in point 41 of the Rules:
    6.1. Take necessary measures to identify the source of the Customer's and Beneficial Owner's funds and assets related to the Business relationship or Transaction;
    6.2. Obtain approval of CEO for establishing or continuing the Business relationship;

6.3. Conduct enhanced ongoing monitoring of the Business relationship by increasing the number and timing of control applied, and by categorising types of Transactions that will need further investigation;

7. It is required to re-establish Customer's identity using enhanced Customer identification procedure if:

   7.1. The Customer knowingly provides wrong information about beneficiary or himself;

   7.2. The Customer hides information.

IX. ASSESMENT OF THE RISK

1. The Company shall assess the risk of the operations being used for money laundering and terrorist financing.
2. The risk assessment shall be conducted on an annual basis.
3. Risk Assessment Procedure provided in Annex No 1 outlines the principal methodology which shall be used to conduct and update the risk assessment for purposes of anti-money laundering and terrorist financing prevention.

X. PERIODIC UPDATE OF CUSTOMER'S INFORMATION

1. By considering the Customer categorisation the Customer's information shall be updated and the Customer's identity shall be verified repeatedly:

   1.1. If the Customer is low risk Customer – every 2 years;

   1.2. If the Customer is medium risk Customer – every year;

   1.3. If the Customer is high risk Customers – every 6 months.

2. The Customer categorisation to the respective risk group shall be registered. When necessary, the data shall be updated.

XI. MONITORING, PRESENTATION OF INFORMATION TO THE FCIS, DETERMINATION AND SUSPENSION OF SUSPECTED MONEY OPERATIONS AND TRANSACTIONS

1. The Company gathers information about the Customer risk profile and expected behaviour when the Customer applies for Company's services. The gathered information provides information about the expected behaviour of the Customer and a baseline for identification of suspicious activity.
2. When suspicious activity is identified, or the Customer otherwise has a suspicious behaviour or pattern that indicates a risk for money laundering, the Company shall seek to investigate the behaviour and to provide a rationale for the identified suspicious behaviour by asking the Customer for additional information to rule out inappropriate behaviour or attempt to launder money. Examples of questions that could be asked:
   - What is the purpose of the requested financing?
   - Where does the income / revenue come from?
   - Why do you want the money to be transferred to this specific account?
   - Etc.
3. The Company has identified indicators, presented below, which shall lead to an inquiry to find out more information about the rationale of the activity. When adequate information about the rationale behind the transaction or behaviours is collected and if the explanation seems reasonable a transaction may be performed. The Company shall notify the FCIS of cases in which the Company:

   3.1. Knows, receives information or has reasonable grounds to suspect that money laundering and / or terrorist financing has been, is being or will be committed or has been attempted;

   3.2. Suspects or has reasonable grounds to suspect that Customer's funds are derived from criminal activity;

   3.3. Suspects or have reasonable grounds to suspect that transactions or activities involve terrorist financing.

4. The Company shall notify the FCIS about the Customer's suspicious (and not only executed, but also intended to be executed suspicious) transactions (irrespective of the size of the monetary transaction),

taking into account:

4.1. Criteria for identifying money laundering and suspicious monetary transactions or transactions related to the Customer behaviour:

a) During the establishment of business relations, the Customer or his representative avoids providing the information necessary to determine his identity, hides the identity of the beneficiary or avoids providing the information necessary for determining the beneficiary, presents documents with doubtful authenticity, etc.;

b) It is difficult to obtain information or documents from the Customer necessary for the monitoring of business relations: it is difficult to contact the Customer, the Customer is often changing its place of residence and contact information; no one responds when trying to call to the phone number provided by the Customer or his representative or it is permanently disabled; the Customer or his representative does not answer e-mails;

c) The Customer is not able to answer the questions asked about his / her financial activity or planned financial activity, its nature, and behaves too nervously;

d) The Customer declares his willingness to end the business relations with the Company when asked to provide the information necessary for monitoring his business relations;

e) The Customer refuses to provide data on the origin of money or attempted to do so and / or to substantiate it by appropriate documents

f) Several companies are registered at the address of the Customer or their representative.

4.2. Criteria related to monetary transactions or transactions executed by the Customer or his representative:

a) Monetary transactions or transactions do not correspond to the regular cooperation with the Company;

b) Customer identification data and information on performed Virtual Currency exchange operations or transactions in Virtual Currency, if the value of such monetary operations or transaction is equal to or exceeds EUR 15,000 or the equivalent amount in foreign or virtual currency notwithstanding whether the transaction is in one or more related monetary transactions. Several interconnected monetary transactions shall be considered to be several Virtual Currency exchange operations or transactions in Virtual Currency in one day, where the total amount of transactions and transactions is equal to or exceeds EUR 15,000 or the equivalent amount in foreign or virtual currency at the time of the transaction;

c) The Customer performs monetary transactions or transactions without a clear economic basis;

d) The Customer performs monetary transactions or transactions where it is difficult or impossible to identify the beneficiary;

e) The Customer, the Customer's representative, a person who is beneficiary of a monetary transaction or transaction, is subject to financial sanctions in accordance with the Law on the Implementation of Economic and Other International Sanctions of the Republic of Lithuania;

f) The age, current position, financial status of the Customer (the Customer's income / revenue is small compared to the amount of his financial activity), objectively does not correspond to the financial activity performed by this Customer.

5. The Company shall inform the FCIS about monetary transactions that do not meet any of the criteria mentioned above, if the Company has a suspicion of a monetary transaction and / or Customer’s activity. The suspicion may be caused by various objective and subjective circumstances, for example, the Customer carries out monetary transactions that are unusual for his activity, provides incorrect information about himself or a monetary transaction, and avoids providing additional information (documents).

6. Suspicious monetary transactions or transactions are objectively determined by focusing on the Customer’s activities that by their nature may relate to money laundering and / or terrorist financing, also by the Customer and beneficiary identification and continuous monitoring of the Customer's Business relationships, including transactions, which were concluded during such relationships. In assessing whether a monetary operation or transaction is suspicious, the Company is not required to determine whether there is a criminal offense. The subjective allegations made by the employee of the Company are sufficient for the assessment.

7. If the employee of the Company finds that a monetary transaction or transaction performed by the

Customer is suspicious, regardless of the amount of such transaction, immediately suspends this transaction and no later than within 3 business hours informs the CEO of the suspended transaction.

8. In case of knowledge or suspicion of suspicious monetary transactions or transactions, the Company shall immediately notify the FCIS, no later than within three working hours after such knowledge or suspicion, if the Company knows or suspects that any value asset is directly or indirectly received from or involved in a criminal offense, also if the Company knows or suspects that the assets is intended to support one or several terrorists or a terrorist organization.
9. The Company, upon receipt of a written instruction from the FCIS to suspend suspicious monetary transactions or suspicious transactions performed by the Customer, suspends these transactions from the time of notification or the moment of the specified circumstances up to 10 business days. The Responsible Employee of the Company submits instructions to the required employees of the Company.
10. If the Company does not receive an obligation to perform a temporary restriction of ownership within 10 working days from the receipt of the prescribed notification or receipt of a written instruction in accordance with the procedure established by the Code of Criminal Procedure of the Republic of Lithuania, the monetary transaction or transaction shall be renewed. The Responsible Employee of the Company submits instructions to the appropriate employees of the Company.
11. Upon receipt of the FCIS notification that the suspension of a monetary transaction or transaction may interfere with the investigation of money laundering or terrorist financing and other criminal acts related to money laundering and / or terrorist financing, the Company shall not suspend suspicious monetary transactions or suspicious transactions performed by the Customer and renew suspended monetary transactions or transactions from the time of notification or the moment of the specified circumstances.
12. A notification to the FCIS regarding a suspicious monetary transaction or transaction shall include:
    12.1. The identity of the Customer, his representative (if the monetary transaction is performed or the transaction is concluded through a representative);
    12.2. Criteria approved by the FCIS, according to which a monetary transaction or transaction is identified as suspicious;
    12.3. A suspicious monetary transaction or a suspicious transaction;
    12.4. The date of the suspicious monetary transaction or the suspicious transaction, the description of the assets in the transaction (money, etc.) and its value (amount of money, currency in which the monetary transaction or transaction is performed, etc.);
    12.5. Account management methods;
    12.6. Contact information (phone numbers, email addresses, contact persons, their telephone numbers, e-mail addresses) of the Customer, his representative (if the monetary transaction is carried out or the transaction is concluded through a representative);
    12.7. The date and time of suspicious monetary operation or suspicious transaction suspension;
    12.8. A description of the assets the Customer cannot manage or use from suspicious monetary transaction or suspicious transaction suspension (location and other information describing the asset);
    12.9. If the suspicious monetary transaction or transaction has not been stopped, – the reasons for not stopping it;
    12.10. Another relevant information in the opinion of the Company.
13. A notification regarding information about suspicious monetary transactions or suspicious transactions shall be submitted to the FCIS upon joining the Information System of FCIS and by filling in an electronic form for providing information on suspicious financial transactions or suspicious transactions approved by the Director of the FCIS (hereinafter – the Information provision form) according to the guidelines for completing the information form approved by the Director of the FCIS.
14. When there is no possibility of joining the FCIS's information system and completing the Information provision form due to technical reasons, and also in urgent cases, the Company may submit information by telephone, fax or e-mail. The information provided on the phone must be described and no later than the next business day after the submission of the information by telephone submitted in writing, fax or e-mail.

XII. REGISTRIES MANAGEMENT

1. The Company shall keep a register of:

   1.1. Monetary transactions and transactions described in the Law;

   1.2. Reported and suspicious monetary transactions or transactions determined in accordance with the criteria given in paragraph XI.53;

   1.3. The Customers with whom transactions or Business relationships were terminated under the circumstances specified in Article 18 of the Law or under any other circumstances related to violations of the procedure for the prevention of money laundering and / or terrorist financing.

2. The Responsible Employee of the Company shall enter the following information into the registries:

   2.1. The data confirming the identity of the Customer, his representative (if any) (first name and surname, date of birth, personal identification number or other unique character assigned to this person for identifying the person / legal entity name, legal form, business address, company code if such code is given).

   2.2. Data on a monetary transaction or transaction – the date of execution of the transaction, description of the assets underlying the transaction (Virtual Currency, money, etc.) and its value (amount of money, currency of a monetary transaction or transaction, etc.);

3. In addition to the data specified in the paragraph 53 of these Rules, the data on the beneficiary (name, surname, date of birth, personal identification code or other unique character assigned to this person, for the purpose of which is given to the person) shall be entered in the registry of suspicious monetary transactions and transactions and also which FCIS approved criteria for identifying the Customer's monetary transaction or transaction as a suspicious transaction or transaction this data meets.

4. Customers' with whom transactions or Business relationships were terminated under the circumstances specified in paragraph 18 of the Law or under any other circumstances related to violations of the procedure for the prevention of money laundering and / or terrorist financing information on the origin of assets, other supplementary data or other information related to violations of the procedures for the prevention of money laundering and / or terrorist financing, the data specified in paragraph 65.1 of these Rules, as well as the data on the beneficiary (name, surname, date of birth, personal identification number or other unique character sequence assigned to this person for identifying him) shall be entered in the registry and also the reasons for which transactions or Business relationships was terminated in circumstances specified in this paragraph and / or in circumstances related to violations of the procedure for the prevention of terrorist financing.

5. The data in the registry shall be recorded in chronological order on the basis of a monetary transaction or transaction according to documents or other legally valid documents related to the execution of monetary transactions or transactions, immediately, but not later than within 3 business days after the execution of a monetary transaction or the conclusion of a transaction except for the case stipulated in paragraph 4, when the data are entered in the registry in chronological order not later than within 7 business days after the occurrence or disclosure of the specified circumstances.

XIII. DATA RETENTION

1. The CEO of the Company is responsible for protecting the data in registries from unauthorized destruction, alteration or use.

2. The registry's data and a copy of the Customer's or beneficiary's identity documents, the live video transmission (live streaming) files and other details obtained at the Customer's identification, accountancy and / or contract documentation (original documents) are kept for 8 years from the end date of transactions or business relations with the Customer.

3. Documents and data confirming a monetary transaction or transaction, or other legally valid documents and data related to the execution of monetary operations or the conclusion of transactions shall be kept for 8 years from the date of the monetary transaction or the conclusion of the transaction.

4. The correspondence of business relations with the Customer shall be kept for 5 years from the date of the closing date of the transactions or business relations with the Customer in paper form or in electronic form.

5. Records of the results of the investigation of complex or unusually large transactions and unusual patterns of transactions specified in Article 17 of the Law shall be stored for 5 years in paper or electronic form.

6. The storage period may be extended for a maximum period of 2 years, when there is a motivated reason provided by the competent authority.
7. The documents and information referred to shall be stored, regardless of whether the monetary transactions or transactions are domestic or international; business relations with the Customer are ongoing or have expired. Moreover, the documents and information referred to shall be stored in such a way as to enable the recovery of specific monetary transactions or transactions, and to provide the information contained therein, if necessary, to the FCIS or other competent authorities.

XIV. INFORMATION PROTECTION AND RESPONSIBILITY

1. Employees of the Company are prohibited from communicating to the Customer or other persons or by other means to let them understand that information about the Customer's monetary transactions or transactions concluded, or the investigation conducted in relation to them, is submitted to the FCIS or to another supervisory authority. This paragraph of the Rules does not prohibit for the Company to:
    1.1. Exchange information between financial institutions registered in the territory of the Member States of the European Union as well as those registered in the territory of third countries which are subject to requirements equivalent to those laid down in the Law if these entities belong to the same group of companies;
    1.2. Exchange information between auditors, accounting or tax advisory services, notaries, notaries representatives and the persons who has the right to perform notarial acts and lawyers and lawyer assistants registered in the territory of the Member States of the European Union and also registered in the territory of third countries subject to requirements equivalent to the requirements set out in the Law if these entities carry out their professional activities as one legal person or as several persons having joint owners and management or as several persons whose activities are subject to general control;
    1.3. exchange information between financial institutions, auditors, accounting or tax advisory services, notaries, notaries representatives and the persons who has the right to perform notarial acts and lawyers and lawyer assistants in cases involving the same Customer and the same transaction involving two or more of the entities referred to in this paragraph if they are registered in the territory of a Member State of the European Union or in the territory of a third country subject to requirements equivalent to those laid down in the Law and if they belong to the same category of profession and have an equivalent level of professional secrecy and personal data protection.
2. In the cases indicated in paragraph 65 of these Rules:
    2.1. The exchange of information is permitted only to prevent money laundering and / or terrorist financing;
    2.2. Exceptions to the transmission of the information provided are not valid if a separate decision of the European Commission has been adopted;
    2.3. When exchanging information with entities registered in third countries and providing personal data to these entities, the provision of personal data must comply with the requirements of the laws protecting personal data.
3. The Company or its employees are not liable for the breach of contractual obligations or damage to the Customer if this is due to a monetary operation or a suspension of a transaction.
4. Employees of the Company who are willing to notify the FCIS of suspicious monetary transactions or transactions executed by the Customer shall not be held liable.

XV. RESPONSIBILITIES

1. The Responsible Employee who carries out the prevention measures specified in the Rules is appointed by the CEO. In cases where a Responsible Employee is unable to perform its tasks, the CEO is considered to be the Responsible Employee.
2. The Responsible Employee of the Company is responsible for:
    2.1. Managing registries;
    2.2. Risk assessment and management;
    2.3. Suspension of suspicious transactions or monetary transactions,

2.4. The implementation of measures to prevent money laundering and terrorist financing; and

2.5. Support of communication with FCIS.

3. The Responsible Employee of the Company has the opportunity to obtain all information necessary for the performance of his functions, including access to information related to identification of the Customer, his representative and beneficiary, information about the Customer's knowledge, monetary transactions and transactions, and other information.
4. The Responsible Employee of the Company shall promptly respond to requests for information from the FCIS and ensure that this information is provided within 14 business days (if the instructions in some cases specify shorter deadlines for the provision of information to the FCIS, such information must be provided within shorter time limits).
5. The Responsible Employee of the Company shall submit a written report at least once a year to the CEO of the Company about the execution of functions related to prevention of money laundering and / or terrorist financing.
6. The Responsible Employee of the Company shall familiarise himself and other employees of the Company with these Rules and with the legal acts regulating prevention of money laundering and liability for the failure to comply with measures of prevention of money laundering.
7. Other employees who find that the transaction may be suspicious, has detected signs of money laundering and / or terrorist financing shall notify the Responsible Employee of the Company who shall take the necessary steps to investigate the operation and inform the CEO and FCIS if necessary.

XVI. FINAL PROVISIONS

1. These Rules may be amended, supplemented or revoked by decision of the CEO of the Company.
2. These Rules shall be reviewed periodically (at least once a year) or upon any substantial events related to the operation of the Company or changes to applicable laws, and shall be amended accordingly to ensure proper implementation of the money laundering and terrorist financing prevention measures, its effectiveness and relevancy. The Responsible Employee is responsible for the timely revision of the Rules and the preparation and submission of draft amendments to the CEO.
3. The Company conducts special training for the employees of the Company on issues related to the prevention of money and terrorist financing, as well as the proper implementation of these Rules.
4. All employees of the Company shall be familiarized with these Rules by signing it.

ANNEXES:

1. Risk Assessment Procedure.

Annex No. 1

RISK ASSESSMENT PROCEDURE

This Risk Assessment Procedure (hereinafter – **the Procedure**) describes the assessment of risk the Company is being exposed to Money Laundering (hereinafter - **ML**) and / or Terrorism Financing (hereinafter – **TF**).

ML/TF risks may occur at different stages taking place one after another or all at the same time: (i) illegal funds are introduced into financial system (placement); (ii) layers of transactions are created to hide the origin of the funds (layering); and (iii) a legitimate purpose is created for the criminal proceeds (integration).

Procedure for conducting an anti-money laundering (hereinafter - AML) and counter terrorism financing (hereinafter - CTF) risk assessment

The Company analyses the risks of ML and TF in context with the most important aspects of the business and the workflows of the Company.

The aim of such analysis is to highlight the factors affecting this risk and to analyse in which stage (placement, layering or integration) the Company is most vulnerable.

The Company's methodology for conducting an AML and CTF risk assessment consists of the following steps:

(a) Analysis of the regulatory acts related to AML/CTF. The review focuses on recent regulatory enforcements for non-compliance with AML and CTF laws and regulations;

(b) Quantitative data is gathered from the Company's business systems such as portfolio data and reviewed with emphasis on changes in the portfolio;

(c) Permanent communication is conducted between employees of the Company with the aim to identify procedural issues or concerns related to AML/CTF as well as to gather insight as input data for the analysis. Moreover, identification of new products or significant changes in processes and procedures are gathered through intense communication with project managers responsible for any recent relevant projects affecting key processes.

(d) Current AML/CTF risk assessment is updated based on gathered information. The risk assessment is updated within, at least, the following areas:

(i) Geography

(ii) Products

(iii) Customers

(iv) Distribution channels

Such areas of risk factors are elaborated below.

1. RISK FACTORS REGARDING THE GEOGRAPHY

1.1. When analysing the risk of ML and TF from a geographical perspective the following factors areas considered:

1.1.1. Negative risk impact factors:

1.1.1.1. If a country is subject of EU sanctions;

1.1.1.2. The country is one of the countries on the list of high risk and other monitored jurisdictions published by and the Financial Action Task Force (http://www.fatf-gafi.org/countries/)

1.1.1.3. The country on the list of third countries with strategic deficiencies in their anti-money laundering and counter-terrorist financing frameworks published by the European Commission

1.1.1.4. Has a weak or non-existent AML/CTF legislation;

1.1.1.5. Has a high Corruption Perception Index.

1.1.2. Positive risk impact factors:

1.1.2.1. Is a member of the European Union or the European Economic Area;

1.2. The Company intends to enter into Business relationships only with the Customers who are residing and having citizenship / are registered in the EU Member State. Thus, the negative factors mentioned in paragraph 1.1.1 will be evaluated upon analysis of (i) the country in which the Beneficial Owners of the Customer reside and (or) have citizenships, (ii) the countries that are Customer's or its Beneficial Owners' main place of business, (iii) the countries to which the Customer and (or) its Beneficial Owners have relevant personal or business links, or financial or legal interests.

1.3. If at least one of the negative risk impact factors described in paragraph 1.1.1 are found to be present, the geographical risk shall be considered to be too high and the Company shall not enter into a business relationship with the Customer.

1.4. If the positive risk impact factors described in paragraph 1.1.2 are found to be present, the geographical risk shall be considered to be low.

1.5. If none of the positive negative or negative risk impact factors described in paragraphs 1.1.1 or 1.1.2 are found to be present, the geographical risk shall be considered to be medium.

2. RISK FACTORS REGARDING THE PRODUCTS

2.1. The Company offers a limited range of services. These products by themselves have limited functionality and are therefore considered to be of a low MT/TF risk.

2.2. The main risk associated is fraud and tax evasion. The Company will take measures to determine the source of fund that the Customer carries out an operation with.

2.3. Overall, given the characteristics of the Company's products, the Company concludes that the Company's products imply a low - medium risk of being used for ML/TF purposes.

2.4. Prior to offering any other product, the Company has to evaluate the risks that they pose and assign a risk category to the product. Areas that have to be assessed prior to the assignment of a risk category to a new product include, but are not limited to:

2.4.1. The level of transparency or opaqueness that the product affords,

2.4.2. The complexity of the product;

2.4.3. The value and size of the product.

3. RISK FACTORS REGARDING THE CUSTOMERS

3.1. Every new customer shall go through the KYC process according to the Rules. Their risk profile is classified as low, medium or high risk for ML/TF based on criteria set out in the Rules.

3.2. Customer negative risk factors which are considered to increase Customer risk are the following:

3.2.1. When Customers legal entities not having legal personality are personal asset-holding vehicles;

3.2.2. When Customer legal entity has nominee shareholders acting for another person, or shares in bearer form;

3.2.3. When Customer legal entity's business is cash-intensive;

3.2.4. When a customer operates in a sector that is associated with a higher ML/TF risk such as casinos or dealers in precious metals;

3.2.5. When the ownership structure of the Customer legal entity appears unusual or excessively complex given the nature of the legal person's business;

3.2.6. The Customer requests transactions that are complex, unusually or unexpectedly large or have an unusual or unexpected pattern without an apparent economic or lawful purpose or a sound commercial rationale;

3.3. The positive factors which are considered to reduce Customer risk are the following:

3.3.1. The Customer that is a legal entity has a clear ownership structure and easily identifiable beneficial owners;

3.3.2. The Customer is a legal person subject to enforceable disclosure requirements that ensure reliable information about the customer and their beneficial owners is publicly available

3.3.3. The Customer is a natural person;

3.3.4. The Customer has been in a long standing business relationship with the Company of no less than 3 years.

3.4. If one or more of the negative risk factors described in paragraph 3.2 are found to be present, the Customer risk shall be considered to be high.

3.5. If none of the negative risk factors described in paragraph 3.2 are found to be present and at least one or more of the negative risk factors 3.2 are found to be present, the Customer risk shall be considered to be low.

3.6. If none of the factors identified in paragraphs 3.2 or 3.2 are found to be present, the Customer risk is considered to be medium.

4. RISK FACTORS REGARDING THE DISTRIBUTION CHANNELS

4.1. All / most of the Company's distribution channels shall be the Company-owned.

4.2. For the performance of KYC duties, the Company may rely on third-service provider. The customer identity is always verified by electronic means. Therefore, the Company's main risk lies in non-compliance from agents about the performance of know-your-customer duties. These duties must be regulated in the written agreements with the agents. Furthermore, the process must be followed closely, and the agents should be informed and possibly also trained by the Company in these matters if the process is not being followed.

4.3. As the Company plans to employ identification methods where the Customer is physically present as well as reliable non-face-to-face identification, in this case the distribution channels shall risk shall be considered to be low where the Customer identification is conducted with the Customer being physically present. In cases the Customer's identity is verified by electronic means, a medium distribution channel risk shall be considered to exist.

5. MEASURES EMPLOYED

5.1. A Customer is considered be a high risk Customer if a high risk is determined to exist in relation to any of the risk categories outlined in sections 1 – 4 of the Procedure. Accordingly, such Customers shall be grouped in the overall high risk category and the Company shall apply an enhanced customer due diligence procedure.

5.2. A Customer is considered to be a low risk Customer if high risk is not determined to exist in relation to any of the risk categories outlined in sections 1 – 4 of the Procedure and if at least 3 low risk factors are determined to exist in relation to the risk categories sections 1 – 4 of the Procedure. Accordingly, such Customers shall be grouped in the overall low risk category.

5.3. The Company shall conduct a ML/TF risk assessment of the Company periodically, but in all cases at least once a year and prior to the introduction of any new product. When conducting a ML/TF risk assessment the Company shall produce a matrix outlining the different categories of risk of each of its customers and review and if necessary update the Rules and the Risk Assessment Procedure.

5.4. If the Company identifies that a risk that has not been identified or is atypical to the current risk assessment exist, the Company shall apply an enhanced customer due diligence procedure.

6. OVERALL ML/TF RISK

6.1. The Company estimates that overall the Company faces a medium vulnerability of being used for ML and TF purposes. However there are risk areas that deserve a more thorough assessment and room to improve the monitoring and mitigation of risks.

6.2. To secure an improved risk management, the Company shall take the following actions:

6.2.1. Securing sufficient Customer knowledge at the point of first contact with new Customers.

6.2.2. Enhancing awareness and knowledge among staff through renewed training and information

sessions by implementing an E-learning solution.

6.2.3. Periodically reviewing and updating the Procedure.