Rules of Internal Control to Avoid Legalization (Laundering) of Proceeds, Money Laundering and Terrorist Financing

1. General

1.1. These Rules of internal control to avoid legalization (laundering) of proceeds of crime and terrorist financing (hereinafter referred to as the "Rules") are established in accordance with the legislation of the location of the Site Operator.

1.2. The Site Operator guarantees to the User that the Operator follows current legislation and international legislative acts in the sphere of counteraction to legalization (laundering) of proceeds of crime and terrorism financing, and shall not deliberately violate the procedure of identification of the User. The Site Operator shall take all necessary measures and technologies in order to provide safe service and service rendering to the Users.

1.3. Using the functions of the Site means the User's unconditional consent to these Rules and the terms of processing their data and other information specified therein. If the User does not agree with the provisions of these Rules, the User has no right to use the Site.

1.4. If the User does not agree to these Terms, the User shall refrain from using the functions of the Site. If any changes are made to these Rules with which the User does not agree, they shall stop using the Site.

1.5. By starting to use any of the features, services and functions of the Site, including browsing the Site pages, regardless of the fact of registration on the Site, the User agrees to these Rules, including any special terms and rules mentioned therein, without any reservations.

1.6. These Rules apply to all registered Users of the Site.

2. Terms and Definitions

Identification means a set of measures of the Site Operator for establishing the information about the Users, determined by the current legislation, for confirming the reliability of this information with the use of original documents and (or) duly certified copies and (or) state and other information systems.

Unusual operation means an operation, which contains possible signs and criteria of uncommonness and which is not typical for the User's operations, as well as any operations, which, in the opinion of the Site Operator's staff, can be carried out for the purpose of laundering proceeds of crime and/or terrorism financing.

Suspicious Operation is an unusual operation which, as a result of internal control measures, raises suspicion that such operation may be carried out for the purpose of money laundering or terrorist financing.

Simplified User Identification - an aggregate of measures to establish the User's full name, first name, patronymic (unless otherwise provided for by law or national custom), series and number of the identity document, and to confirm the accuracy of such information by one of the following methods:

- Using original documents and (or) duly certified copies of documents;
- Using information from information systems of public authorities;

Internal Control - implementation of internal control rules by the Site Operator, including but not limited to meeting legal requirements for identification of Users, recording information (data) in a documentary format and storage of documents and information.

3. Purpose, Tasks and Basic Requirements of Internal Control

3.1. Internal control shall be exercised to ensure compliance with the requirements of applicable laws and other international acts and shall be aimed at identifying and managing the risks associated with money laundering and terrorist financing.

3.2. The tasks of internal control are as follows:

3.2.1. preventing the Site Operator from being involved in money laundering and terrorist financing;

3.2.2. ensuring the implementation and observance of these Regulations by all the Site Operator's employees, subject to the following requirements:

- participation in the internal control process of all employees regardless of their position within their competence;
- observance of banking secrecy and preservation of confidentiality of information obtained in the course of performing internal control;
- exclusion of participation of the Site Operator's employees in money laundering and terrorism financing;
- making sure that the Users and other persons are not informed about measures taken by the Site Operator in the course of performing internal control, except for informing Users about suspension of operation, about refusal in execution of User's instruction regarding performance of operations;
- keeping confidentiality of information about the internal documents of the Site Operator.

3.3. Application of effective procedures for evaluation of risks, connected with money laundering and terrorism financing.

3.4. The Site Operator works on the Site structure in order to ensure compliance with regulatory requirements and at different levels both locally and globally, and to ensure continuous operation of the Site.

3.5. The Site Operator collects and processes said data in order to be able to:

- comply with legal and regulatory obligations, as applicable;
- conduct internal audits as well as other due diligence checks;
- confirm the identity or claimed identity of the User and identify and/or verify the source of the User's funds, as applicable;
- conduct a risk assessment with respect to potential Users and Affiliates;
- execute any legal or regulatory obligation that the Site Operator may have.

4. User Identification

4.1. The Site Operator understands that identification of Users and anti-money laundering policy is a complex system of international policy and in this connection the Operator takes all necessary measures for identification of Users.

4.2. The information requested from the User refers to:

- Surname, first name and patronymic (if any).
- Date of birth.
- Nationality.
- Details of the identity document: series (if any) and number of the document, date of issue of the document, name of the issuing authority and subdivision code (if any).
- Address of residence (registration) or place of stay.
- Contact information (e.g. telephone number, fax number, e-mail address, mailing address, if any).

4.3. In case of Simplified Identification of the User when transferring funds at the User's request without opening a bank account, including electronic funds, as well as when providing the User with an electronic means of payment:

- Surname, first name and patronymic (unless otherwise provided by law or national custom).
- Details of the identity document: series and number of the document, date of issue of the document, name of the issuing authority and subdivision code (if any).
- Other information, allowing to confirm the specified information.

4.4. The Site Operator identifies Users when carrying out transactions with NFTs.

5. Control over Users' Operations and Transactions in the Register

5.1. The Site Operator establishes and has the right to adjust the daily transaction limit depending on the security and actual situation of the transaction.

5.2. The Site Operator shall evaluate and decide whether the operation is unusual or suspicious. The operator at its discretion decides that the operation is suspicious.

5.3. The Site Operator shall:

5.3.1. Develop internal transaction monitoring and control procedures, such as identity verification by technical means;

5.3.2. Carry out due diligence and continuous surveillance of Users, using risk prevention methods;

5.3.3. Review and regularly verify the transactions performed;

5.3.4. Report of any suspicious transactions to competent authorities.

5.4. Transactions that contain information about:

- types of virtual financial assets involved, order volume, price, value;
- transaction history on the Site; and
- portfolio data, which includes information on virtual financial assets and amounts credited to the digital wallet in the User's Account, and balances of the digital wallet in the User's Account.

6. Identification of User's Operations subject to Mandatory Control

6.1. The Site Operator's employees shall identify transactions subject to mandatory control and unusual transactions within the scope of their functional duties.

6.2. If there are the grounds for classifying the User's operation as one subject to mandatory control, the Operator's employee shall make a decision to recognize the User's operation as subject to mandatory control.

6.3. The grounds for qualifying an operation as suspicious are:

- confusing or unusual nature of the operation (transaction), which has no obvious economic sense or obvious legitimate purpose;
- identification of repeated transactions (deals), the nature of which gives grounds to believe that their purpose is to evade mandatory control procedures;
- the suspicion of carrying out a cash transaction connected with the financing of terrorism;
- other circumstances giving ground to believe that the transactions (deals) are conducted for the purpose of money laundering or financing of terrorism.

6.4. If any unusual transactions (deals) have been identified, the Site Operator's employee shall take the decision about further actions of the Site Operator in respect of the User and his transaction (deals).

6.5. The identification criteria and characteristics of unusual transactions (deals) are not exhaustive. A transaction can also be recognized as unusual based on the analysis of the nature of the transactions, its components, accompanying circumstances and interaction with the User, even if the transaction does not formally meet the criteria for identifying and recognizing unusual transactions.

7. Confidentiality

7.1. This Procedure ensures confidentiality of any information and documents related to performance by the Site Operator of anti-money laundering and anti-terrorist financing measures.

7.2. The confidentiality of the information is provided in accordance with the Privacy Policy, posted on the Site.

7.3. To ensure confidentiality, access to information resources containing information is strictly limited and controlled.

7.4. Organization of access to the relevant information systems of the Site Operator, procedure for handling confidential information, actions of responsible contractors and officials, as well as their interaction in securing information shall be performed in accordance with these Rules.