AML and KYC POLICY

Date of last update: 11.03.2021

1. **GENERAL PROVISIONS**

1.1. This Policy defines the basic principles for the organization and operation of the internal control system in the Cryptostreet OU (Cryptostreet OÜ) Company (registration number 14711680) for anti-money laundering (AML) and the financing of terrorism (CFT). In this regard, the Company is implementing a set of measures aimed at identifying and combating money laundering in accordance with international requirements for this aspect.

1.2. The objectives of this Policy are:

1) creating a basis for the formation of an internal regulatory framework in the field of AML;

2) identification of key values and elements in AML/CFT issues.

1.3. The implementation of the Policy in the Company is ensured by the relevant internal rules, procedures, as well as organizational and administrative measures and management decisions.

2. PRINCIPLES OF THE INTERNAL CONTROL ORGANIZATION

2.1. The principle of compliance with norms and international requirements.

The Company forms and implements internal control procedures for money laundering and terrorist financing to the extent necessary and in accordance with international requirements.

The Company also requires counterparties and clients to strictly adhere to and comply with the rules and procedures approved by the Company as part of internal control.

The Company does not participate and reacts properly to any facts that have become known to it about actions on the part of the System participants aimed at using prohibited practices such as bribery, coercion, collusion, fraud, contributing to the legalization (laundering) of proceeds from crime and the financing of terrorism.

2.2. Know Your Client (KYC) Principle

According to AML and KYC (Know Your Client) policies, the Company takes measures for due verification of clients, including through their identification and verification when establishing contractual relations and conducting transactions in the Company's system. The company verifies the client in case of doubts about the reliability of previously received information.

During the registration process, the client provides the Company with the data necessary for his/her authentication in the system.

During the verification process, the client provides his/her identifying information which includes the full name of the Client, date of birth, country of residence, phone number and (or) e-mail and other data.

After receiving identifying information, the Company verifies the Client by requesting the relevant documents.

The document intended to verify the identity of the Client is a high quality scanned copy or photo of the passport.

Additionally, the Client provides documents confirming the residential address in accordance with the requirements specified on the Company's website: cryptostreet.me.

The Company has the right to instruct another person to conduct the client identification and (or) verification procedure. At the same time, the Client provides such a person with his/her consent to the collection, processing, storage and transfer of personal data. The Company's Clients also give consent to the collection, processing, analysis and use of personal information by the Company and take an active part in KYC procedures ensuring proper verification and financial monitoring.

The Company conducts regular comprehensive verification of the client and client's accounts in order to determine the risk he/she may bear and to identify changes in the information about the client.

The Company continuously monitors the actions of the clients in the system in order to identify suspicious transactions that require an appropriate response in accordance with international requirements.

If the Company believes that cooperation with the client has a high risk of money laundering or terrorist financing, the Company has the right to request any other additional documents that it deems necessary in this situation.

The Client is obliged to immediately report any changes in personal information or contact details.

2.3. Principle of zero tolerance for the risk of money laundering and terrorist financing

The Company manages the risk of legalization (laundering) of proceeds from crime and financing of terrorism within the framework of the common risk management system by setting a high level of danger for the system based on the understanding that these types of illegal acts are serious crimes that threaten the stability and security of the society and state.

Based on an objective assessment of the available resources and real opportunities, the Company takes the maximum legal and technically possible measures to counter the legalization (laundering) of proceeds from crime and financing of terrorism.

The Company applies restrictions and sanctions to the clients who deliberately violate or avoid internal control procedures for AML purposes, as well as those caught in dubious or explicit actions in the Company's system that fall under the signs of legalization (laundering) of proceeds from crime and financing of terrorism up to blocking access to the system, terminating contractual relations and transferring information to authorized state bodies.

3. PAYMENT POLICY

3.1. To minimize the risk of money laundering and terrorist financing, the Company does not accept or pay cash under any circumstances.

3.2. The Company reserves the right to suspend, refuse to process a transaction, conduct an operation in the system at any stage in the event of the assumption that the transaction / operation is in any way related to money laundering or criminal activity.

3.3. According to international law, the Company does not inform the client that the relevant authorities have been notified of his/her suspicious activity.

3.4. When replenishing a personal account in the system, the name of the sender of funds must fully correspond to the name specified when registering the account. Third party payments are not accepted.

3.5. Money can be withdrawn to the same account and in the same way as the deposit was made.

3.6. The Company stores data on all transactions, operations of the client for five (5) years from the date of termination of the business relationship.

4. FINAL PROVISIONS

4.1. Responsible for compliance with this Company Policy is the designated Money Laundering Compliance Officer who is responsible for the Company's compliance with AML and KYC policies, for the development and implementation of AML and KYC procedures of the Company, training of employees in the area of money laundering prevention, monitoring of client transactions, reviewing internal reports of suspicious activity, etc.

4.2. The Company has the right to change this AML Policy at any time and in connection with this, the continued use of the Company's services by the client means the acceptance of the changes to this Policy.