MONEY LAUNDERING AND TERRORIST FINANCING PREVENTION POLICY

OBJECTIVE AND BASES OF POLICY

The legal basis of this Policy is the legislation of the Republic of Estonia and the European Union, international agreements and conventions, instructions of international organisations and regulatory authorities.
The objective of the Policy is to establish the basic principles and general activity guidelines in order to ensure efficient and proportionate implementation of money laundering and terrorist financing prevention measures at CoinEx Group OÜ, hereinafter the Company.
The Company was founded on 12.12.2002, the Company's website is at https://coinex.cash/. The money laundering and terrorist financing prevention activities are organised by and are the responsibility of a member of the Management Board of the Company or the Financial Intelligence Unit Compliance Officer appointed by a member of the Management Board.

The Company's risks and the measures for mitigating these are determined by the Risk Assessment; the Company's risk appetite is also determined in the Risk Assessment.

The Company is guided upon prevention of the money laundering and terrorist financing by the principle of Know Your Customer. One of the primary prerequisites for the efficient functioning of the principle of Know Your Customer is the gathering of as precise and as thorough data as possible upon establishment of the customer relationship. This enables, based on the data provided by the customer, to position the customer's initial degree of risk and assess the compliance of the customer's payment behaviour with the data provided thereby.
The risk-based approach, gathering and updating of data, monitoring of transactions and analysing documents certifying the origin of property are the measures whose implementation must result in the creation for the Company of a full picture of the customer and the Company's inner belief that the customer's activities are legal.
The Company implements the principle of Know Your Customer during the entire customer relationship. The Company assesses and analyses the risks of money laundering and terrorist financing on a regular basis and has established detailed instructions to the employees of the Company for money laundering and terrorist financing prevention.

The specific instructions for the prevention of money laundering and terrorist financing are determined in the guideline “Procedures to prevent money laundering and terrorist financing”.
The employees of the Company are obliged to fully comply with the instructions for prevention of money laundering and terrorist financing established in the legislation and the internal rules.

COMPANY'S AREAS OF ACTIVITY

The company operates on the basis of licences issued by the Money Laundering Bureau (RAB) and is under the supervision of RAB. The company provides the following services:
1. currency exchange, licence number VVT000337
2. pawnshop services (loan secured by gold), licence number FIP000170
3. virtual currency wallet service, licence number FVT000080
4. exchange of virtual currencies through BATM and at the representative office of the Company, licence number FVT000080
5. operating as a financial institution, licence number FFA000144.

All services are provided only when physically present in the same place as the person, i.e. in the Company's offices, and all persons are identified regardless of the size of the transaction amount (except currency exchange in cash up to 1000 euros). The company does not offer virtual currency payment services to its customers. The company's offices are located in Tallinn at Tartu mnt. 51-3A and Laikmaa 5 and in Tartu at Küüni 7.
Using BATM, it is possible to make transactions only in cash, the CRM program of BATM allows one customer to make transactions within the limit of up to 1000 euros.

RISK MANAGEMENT SYSTEM

All employees must ensure the identification of risks in the activities, products and processes in their sphere of responsibility, assessment thereof and implementation of sufficient control mechanisms to identify any deficiencies and errors in the activities of the employees, job descriptions, procedures or processes. In order to ensure compliance with this principle, the Company has divided the risk management tasks according to the international method of three lines of defence.

1st line of defence

The first line of defence is the CRM program and customer service representatives, whose tasks are to apply due diligence measures when establishing a business relationship, including identifying the customer's identity and applying the know-your-customer principle in such a way that, based on the information received, it is possible to determine the customer's risk profile and degree of risk and subsequent monitoring of the business relationship. The work of the program is controlled by the RAB contact person and internal control.

2nd line of defence

The second line of defence is formed by the responsible board member and RAB contact person.

The responsible member of the board ensures the identification, assessment and management of risks related to the company's processes/products/services, including organizing the mapping and analysis of risk factors to assess the suitability of existing measures to prevent money laundering and terrorist financing, and is responsible for the existence of internal regulations that comply with legislation and supervision instructions. RAB's contact person has a reporting obligation to the board once every six months. The task of the RAB contact person is to collect information on unusual transactions suspected of money laundering and/or of a nature indicative of terrorist financing, analyzing the relevant information and, if necessary, forwarding it to the Financial Intelligence Unit and fulfilling the latter's instructions and training employees. The RAB contact person is also responsible for fulfilling the obligations arising from the international sanctions law.

3rd line of defence
The third line of defence is formed by the company's auditor, who carries out the audit of the annual report and the control of compliance with the established requirements for own funds, and submits a relevant opinion to both the Company and the Money Laundering Data Office by the deadline for submitting the annual report, and the internal auditor, who regularly checks the compliance of the board, RAB contact person, customer services and IT solutions with legislation , to the requirements stipulated in the supervision instructions and the internal rules of CoinEx Group OÜ. The internal audit makes proposals to the management board to eliminate deficiencies revealed during the inspection and to change and supplement internal procedures.

ASSESSMENT OF RISKS

By constant assessment of risks the Company tries to minimise the possibility that its services could be used for money laundering or terrorist financing. Annual and *ad hoc* risk assessments are documented and made available to the employees and, if necessary, to the regulatory authorities.

The measures adopted for the identification, assessment and analysis of risks must comply with the nature and complexity of the business activities. After the assessment of risks, such measures must be prescribed by which the risks are efficiently mitigated. The main risk factors, how high is the probability of their realisation, and to what extent due diligence measures have to be applied for mitigating the risks are established during risk assessment. Peamiseks rahapesu ja terrorismi rahastamise alaste riskide maandamise meetmeks on hoolsusmeetmete proportsionaalne ja riskipõhine kohaldamine. Riskide efektiivseks juhtimiseks ja maandamiseks on äärmiselt oluline töötajatele operatiivsete juhiste andmine.

In order to assess risks, information is gathered about the customers which allows them to determine the customer profile and understand the risks associated with the customer and the transactions of the customer. When identifying the risks, different risk categories

are taken into consideration in the aggregate and the degree of risk is determined for the customer. The scope of the due diligence measures applicable to the customer depends on the degree of risk of the customer.

Determination of the degree of risk is based on predetermined criteria based on which customers of low, medium and high degree of risk are determined, determining also the customers and services for which the application of simplified or usual due diligence measures is sufficient and the customers and services for which it is necessary to apply enhanced due diligence measures.
The determination and changing of the degree of risk requires continuous monitoring of the business relationship, including analysis of the transactions conducted during the business relationship in order to ensure that the transactions conducted are in line with the Company's knowledge about the customer, the customer's activities and their compliance with the criteria of the degree of risk assigned to the customer.

DUE DILIGENCE MEASURES

Depending on the customer's risk profile the Company applies either usual or enhanced due diligence measures. The bases for the selection of due diligence measures and the scope of their application have been determined by the Company in the Risk Assessment. Detailed instructions to the employees of the Company for applying due diligence measures are established in the guideline “Procedures to prevent money laundering and terrorist financing”.
The Company uses a risk-based approach upon application of due diligence measures, observes the principle of Know Your Customer and conducts continuous monitoring of the customers and transactions.
The Company ensures that all employees pass training on the prevention of money laundering and terrorist financing before commencement of work and provides subsequent training to them based on necessity, but not less frequently that once annually.

CUSTOMER PROFILE EXCLUSIONS

The Company has determined a number of criteria and characteristics in the customer profile which preclude the establishment of a business relationship with the person by the Company:

1. with persons in respect of whom it is not possible to carry out due diligence measures;
2. with persons about whom money laundering and/or terrorist financing is previously known or suspected during the application of due diligence measures;
3. with anonymous and/or fictitious persons and shadow persons;

4. with shadow banks and such credit institutions or financial institutions that are known to allow shadow banks to use their accounts (correspondence relationships are not established);
5. with sanction subjects - with persons included in the UN, OFAC and EU sanctions lists;
6. with natural or legal persons originating from FATF risk countries (where sufficient measures to prevent money laundering and terrorist financing are not implemented);
7. with tumbler/mixer service providers;
8. with persons whose capital consists of more than 10 percent of issuer shares or other issuer securities;

UPDATING OF POLICY

The Management Board of the Company examines the compliance of the Money Laundering and Terrorist Financing Prevention Policy with the legislation, the Company's economic results and risk management model annually and updates the Policy, if necessary.