

## KYC/AML POLICY

The terms used in this KYC/AML Policy shall have the same meanings as in the Terms of Use except as otherwise specified.

Please read this Know-Your-Customer/Anti-Money Laundering (“KYC/AML”) Policy carefully before using neocrypto.net website and our Services. You should read and understand it before accessing the Services, because this AML/KYC Policy is one of the documents that allow the Client to use the Services of Neocrypto correctly and safely. If you are in any doubt about any of the contents of this document, you should obtain independent professional advice.

### 1. General provision

This KYC/AML Policy lays down requirements for identification, verification, screening and ongoing monitoring of our Clients and their transactions in order to prevent crime, money laundering, terrorist financing, sanctions or tax evasion, and to ensure identification and reporting of such cases.

This KYC/AML Policy is an excerpt of our internal Anti-money laundering and counter terrorist financing Policy (“Policy”) and is primarily based on the regulations set out in Republic of Lithuania Law on the Prevention of Money Laundering and Terrorist Financing (Law) and other applicable legislation.

The requirements of this Policy apply to all actions that are provided for by the Terms of Use published on the website <https://neocrypto.net>.

### 2. Definitions

Money Laundering (hereinafter ML) – is a set of activities with the property derived from criminal activity or property obtained instead of such property with the purpose to conceal or disguise the true nature, source, location, disposition, movement, right of ownership or other rights related to such property; convert, transfer, acquire, possess or use such property for the purpose of concealing or disguising the illicit origin of property or of assisting a person who is involved in criminal activity to evade the legal consequences of his or her action.

Terrorist Financing (hereinafter TF) – means the financing and supporting of an act of terrorism and commissioning thereof as well as the financing and supporting of travel for the purpose of terrorism in the meaning of applicable legislation.

International Sanctions – list of non-military measures decided by the European Union, the United Nations, another international organization, the government of the Republic of Lithuania and aimed to maintain or restore peace, prevent conflicts and restore international security, support and reinforce democracy, follow the rule of law, human rights and international law and achieve other objectives of the common foreign and security policy of the European Union.

Money Laundering Reporting Officer (MLRO) – representative appointed by the Management Board responsible for the effectiveness of the AML/CTF Policies, conducting compliance over the adherence to the relevant policies and serving as contact person of the FCIS.

FCIS - Financial Crime Investigation Service of Lithuania.

Business Relationship – a relationship established by Neocrypto in its economic and professional activities with the Client.

Client – a natural person, who uses services of Neocrypto.

Transaction – an exchange of fiat currency against virtual currency conducted by the Client through Neocrypto.

Beneficial Owner – is a natural person, who:

- Taking advantage of his influence, exercises control over a transaction, operation or another person and in whose interests or favor or on whose account a transaction or operation is performed.
- Ultimately owns or controls a legal person through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that person, including through bearer shareholdings, or through control via other means.
- Holds the position of a senior managing official, if, after all possible means of identification have been exhausted.
- In the case of a trust, civil law partnership, community or legal arrangement, the beneficial owner is the natural person who ultimately controls the association via direct or indirect ownership or otherwise and is such association.

Neocrypto – UAB Effective Global Solutions, company registry code: 305970282, company registered address: Vilnius, Eišiškių Sodų 18-oji g. 11, Lithuania. Effective Global Solutions UAB is authorised by the FCIS of the Republic of Lithuania to provide virtual currency exchange operator services.

Politically Exposed Person or PEP - is a natural person who is or who has been entrusted with prominent public functions, or his or her close relative or associate, including heads of international organizations.

Management Board or MB – management board of the Company. Member of the MB, as appointed by relevant MB decision, is responsible for implementation of the AML/CTF policies and procedures.

Equivalent Third Country – means a country not a Member State of the European Economic Area but applying an equivalent regime to the European Union corresponding (AML) framework.

Virtual currency - a value represented in the digital form, which is digitally transferable, preservable or tradable and which persons accept as a payment instrument, but that is not the legal tender of any country.

### 3. Money Laundering Reporting Officer (MLRO)

The MB appointed an MLRO whose principal tasks are to monitor the compliance of the Policy with the relevant laws and regulations; compile and keep updated the data regarding countries with low tax risk, high and low risk of ML and TF and economical activities with great exposure to ML and TF; instruct and update the staff; report to the MB on compliance with the Policy; collect, process and analyze the data received from staff or Clients concerning suspicious and unusual activities; receive internal disclosures, make reports and collaborate with the FCIS on events of suspected ML or TF; make proposals on remedying any deficiencies identified in the course of checks.

### 4. Application of due diligence measures

Neocrypto shall determine and take due diligence (hereinafter DD) measures using results of conducted risk assessment, and provisions of national risk assessment, published on the web page of the Ministry of Finance of Lithuania.

DD measures shall include the following procedures:

- Identifying the Client and verifying its identity using reliable, independent sources, documents or data, including e-identifying;
- Identifying and verifying of the representative of the Client and the right of representation; ● Identifying the Client's Beneficial Owner;
- Assessing and obtaining information on the purpose of the Business Relationship; ● Conducting ongoing DD on the Client's business to ensure the Provider of service's knowledge of the Client and its source of funds is correct;
- Obtaining information whether the Client is a PEP or PEP's family member or PEP's close associate;
- Obtaining information whether International Sanctions are imposed against the Client, Beneficial Owner, representative, director and other persons that may be relevant.

To comply with the DD obligation, Neocrypto have the right and obligation to:

- request documents and information regarding the activities of the Client and legal origin of funds;
- request appropriate identity documents to identify the Client and its representatives; ● request information about Beneficial Owners of a Client;
- screen the risk profile of the Client, select the appropriate DD measures, assess the risk whether the Client is or may become involved in ML or TF;
- re-identify the Client or the representative of the Client, if there are any doubts regarding the correctness of the information received in the course of initial identification;
- refuse to participate in or carry out the Transaction if there is any suspicion that the Transaction is linked with ML or TF, or that the Client or another person linked with the Transaction is or could be involved in ML or TF.

The objective of the continuously applied DD measures is to ensure on-going monitoring of Clients and their Transactions.

Neocrypto updates the data of a Client, i.e. takes appropriate DD measures, every time when:

- upon identification and verification of the information;
- based on data renewal terms which may vary depending on the risk group to which particular Client is assigned to;
- Neocrypto has learned through third persons or the media that the activities or data of the Client have changed significantly;
- the data pertaining to the Transactions of Client reveal significant changes in the Client's area of activity or business volumes, which warrants amending the Client's risk profile.

#### 5. Identification of a person

Neocrypto provides its services to individual Clients (national persons) only.

Upon implementing DD measures the following person shall be identified:

- Client – a natural person;

- Representative of the Client – an individual who is authorized to act on behalf of the Client; ● Beneficial Owner of the Client;
- PEP – if the PEP is the Client or a person connected with the Client.

Upon establishing the relationship with the Client Neocrypto shall identify and verify the Client by using information technology means, and follow technical requirements for the customer identification process for remote identification authentication via electronic devices for direct video transmission.

- Consequences of insufficient identification of a Client:
- Promptly apply the enhanced DD measures pursuant to the Policy;
- Notify the MLRO of the failure to implement normal DD in a timely manner; ● Assess the risk profile of the Client and notify MLRO and/or MB;
- Suspicious Transactions should be monitored and assessed postnote.

#### 6. Establishing the purpose and actual substance of a Transaction

In order to screen out suspicious or unusual Transactions and the purpose and actual substance of a Transaction, Neocrypto shall take the following actions:

- request additional information from the client about the professional or economic activities when making a Transaction above certain limits;
- ask the Client explanations about the reasons for the Transaction and, if necessary, documents evidencing of the origin of the assets and/or source of wealth;
- being particularly attentive to Transactions, which are linked with natural or legal persons, whose country of origin is a state, wherefrom it is particularly difficult to receive information about the Client and/or transactions with persons, who originate from such states, which do not contribute sufficiently into prevention of ML.

#### 7. Risk assessment

Neocrypto conducts risk-assessment of its activities and Clients, and establishes a risk profile of a Client based on information gathered under the Policy and applies relevant levels of due diligence measures accordingly.

#### 8. Prohibited Transactions

The Client shall use Neocrypto's Services solely in compliance with its Terms of Use, including this KYC/AML Policy, solely for his or her own account. The Client shall not sell, lease or otherwise provide access to the Services to any third party.

The following conduct and Transactions are prohibited:

- The Client does not have sufficient authorizations to carry out the Transaction, or the authorizations are unclear;
- The Client's need to carry out the Transaction has not been reasonably justified; ● The Client is a fictitious person;
- The Client or the representative of the Client refuses to provide information for the purposes of establishing the substance of the Transactions and assessment of the risks;

- The Client has not presented sufficient data or documents to prove legal origin of the assets and funds, after having been asked to do so;
- Based on the information received from recognized and reliable sources (e.g. state authorities, international organizations, media) the Client, the Beneficial Owner of a Client, or another person associated with the Client (e.g. director, representative) is or has been linked with organized crime, ML or TF, tax evasion, bribery or corruption;
- The Client, the Beneficial Owner of a Client, or another person associated with the Client is or has been linked with sources of income of organized crime, i.e. illicit traffic of excise goods or narcotic substances, illegal trafficking of arms or human trafficking, mediation of prostitution, unlicensed international transfers of e-money;
- International Sanctions are being applied against the Client, the Representative or the Beneficial Owner;
- The Client advocates, promotes or assists any violence or any unlawful act.

## 9. Storage of data

The data is stored in a written format and/or in a format reproducible in writing and, if required, it shall be accessible by all appropriate staff of the Company.

The originals or copies of the documents, which serve as the basis for identification of a person, and of the documents serving as the basis for establishing a Business Relationship, shall be stored for at least eight (8) years after the expiry of the Business Relationship or the completion transaction.

Information regarding Transactions reported to the FCIS shall be stored by the MLRO and shall be accessible only to MB.

## 10. Reporting of suspicious Transaction

Notification of the MLRO:

Any circumstances identified in the Business Relationship are unusual or suspicious or there are characteristics which point to ML, TF, or an attempt of it, shall promptly escalate to the MLRO.

The MLRO shall analyze and forward the respective information to the MB.

Notification of the FCIS:

The MLRO shall decide whether to forward the information to the FCIS and the MB shall decide whether to terminate the Business Relationship.

It is prohibited to inform any third persons, including other staff of Neocrypto, of the fact that information has been reported to the FCIS, and the content of the reported information, except for the MB/MLRO.

## 11. Implementation of International Sanctions

Neocrypto is required to implement International Sanctions in force.

Neocrypto conducts screenings and draws special attention to all its Clients (existing and new), to their

activities and to the facts and indicators which refer to the possibility that the Client is a subject to International Sanctions in force.

## 12. Restricted jurisdictions

Albania, Afghanistan, The Bahamas, Barbados, Botswana, Burkina Faso, Cambodia, Cayman Islands, Cuba, Democratic Republic of Korea (DPRK), Haiti, Ghana, Jamaica, Iran, Iraq, Gibraltar, Mauritius, Morocco, Myanmar, Nicaragua, Pakistan, Panama, Philippines, Senegal, South Sudan, Syria, Trinidad and Tobago, Uganda, Vanuatu, Yemen, Angola, Burundi, Central African Republic, Congo, Congo (Democratic Republic of the), Guinea-Bissau, Liberia, Lybia, Mali, Sierra Leone, Somalia, Côte d'Ivoire, the United States of America (USA), United Kingdom (UK), Zimbabwe, Russian Federation if a Client is not a long-term resident of the European Economic Area (EEA) or a citizen of an EU member state, unrecognized countries or territories.

Neocrypto reserves the right to choose markets and jurisdictions in which it operates, and may also restrict or refuse provision of its services in other countries, territories or regions if deemed necessary by its own risk appetite or required by laws, competent authorities or sanctions programs. You should inform us immediately if you become a citizen or a resident in any of the Restricted jurisdiction. You understand and acknowledge that if it is determined that you have given false representations of your location or place of residence, Neocrypto reserves the right to take any appropriate actions with compliance to the local jurisdiction, including termination of your access to Neocrypto's Services.

IF YOU HAVE ANY QUESTION REGARDING PRESENT AML/KYC POLICY OR OUR POLICY OR NEED ANY ADDITIONAL DETAILS / INFORMATION / EXPLANATIONS, PLEASE CONTACT US DIRECTLY.