Last update: "12" December 2023

AML POLICY

This Anti-Money Laundering Policy (“Policy”) is an agreement between you (“User”, “You") and Web4 Solutions Limited, company registration code: 239845, legal address of the company: Suite 3, 1st Floor, La Ciotat Building, Mont Fleuri, Mahe, Seychelles ("Company", " We ").

1. General provisions

1.1. The terms used in this Policy must have the same meanings as in the Terms of Use (“Agreement”), except where otherwise specified.

1.2. Please read this Policy carefully before using the site https://demi.gg (“Site”) and our services (“Services”).

1.3. You should read and understand this Policy before accessing the Services, because this Policy is one of the documents that allow the User to use the Services correctly and safely. If you have any doubts about the contents of this document, you should seek independent professional advice.

1.4. This Policy sets out requirements for the identification, screening and continuous monitoring of our Users and their transactions in order to prevent crimes, money laundering, terrorist financing, sanctions or tax evasion, as well as to ensure the detection of such cases and reporting on them.

1.5. The requirements of this Policy apply to all actions provided for by the Agreement published on the Site.

2. Definitions

2.1. Money Laundering (hereinafter ML) – 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 the property or of assisting a person who is involved in criminal activity to evade the legal consequences of his or her action.

2.2. Terrorist Financing (hereinafter TF) – means the financing and supporting for 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.

2.3. International Sanctions – list of non-military measures decided by the United Nations, another international organization, aimed at maintaining or restoring peace, preventing conflicts and restoring international security, supporting and strengthening democracy, observing the rule of law, human rights, and international laws.

2.4. Money Laundering Reporting Officer (MLRO) – a representative appointed by the Management Board, responsible for the effectiveness of the Policy.

2.5. Business Relationship – a relationship established by the Company in its economic and professional activities with the User.

2.6. User – a natural person who uses Services.

2.7. Transaction – an exchange of fiat currency against virtual currency conducted by the User through the Company.

2.8. Beneficial Owner – 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 partnership, community or legal agreement, the Beneficial owner is an individual who ultimately controls the association through direct or indirect ownership or otherwise and is such an association.

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

2.10. Virtual currency - a value represented in 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)

3.1. The Company appoints a Money laundering reporting officer whose main tasks are:

- monitoring the compliance of the Policy with relevant laws and regulations;
- collection and continuous updating of data on countries with low tax risk, high ML and FT risk, as well as economic activities subject to ML and FT;
- staff briefing and training;
- reporting to the Company on compliance with the Policy;
- collection, processing and analysis of data received from employees or Users regarding suspicious and unusual actions;
- obtaining internal information, compiling reports; making proposals to eliminate any shortcomings identified during inspections.

4. Application of due diligence measures

4.1. The Service shall determine and take due diligence (hereinafter DD) measures using results of the conducted risk assessment.

4.2. DD measures shall include the following procedures:

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

4.3. To comply with the DD obligation, the Company has the right and obligation to:

- request documents and information regarding the activities of the User and legal origin of funds;
- request appropriate identity documents to identify the User and its representatives;
- request information about Beneficial Owners of a User;
- screen the risk profile of the User, select the appropriate DD measures, assess the risk whether the User is or may become involved in ML or TF;
- re-identify the User or the representative of the User, 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 User or another person linked with the Transaction is or could be involved in ML or TF.

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

4.5. The Company updates the data of a User, 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 User is assigned to;
- The Company has learned through third persons or the media that the activities or data of the User have changed significantly;
- the data pertaining to the Transactions of the User reveal significant changes in the User's area of activity or business volumes, which warrants amending the User's risk profile.

5. Identification of a person

5.1. Upon implementing DD measures the following person shall be identified:

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

5.2. Upon establishing the relationship with the User the Company shall identify and verify the User 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.

5.3. Consequences of insufficient identification of a User:

- Promptly apply the enhanced DD measures pursuant to the Policy;
- Assess the risk profile of the User and notify MLRO and/or MB;
- Suspicious Transactions can be monitored andevaluated ex post facto .

6. Establishing the purpose and actual substance of a Transaction

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

- request additional information from the User about the professional or economic activities when making a Transaction above certain limits;
- ask the User 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 User and/or transactions with persons, who originate from such states, which do not contribute sufficiently into prevention of ML.

7. Risk assessment

7.1. Company conducts risk-assessment of its activities and Users, and establishes a risk profile of a User based on information gathered under the Guidelines and applies relevant level of due diligence measures accordingly.

8. Prohibited Transactions

8.1. The User shall use the Service solely in compliance with its Agreement, including this Policy, solely for his or her own account. The User shall not sell, lease, or otherwise provide access to the Services to any third party.

8.2. The following conduct and Transactions are prohibited:

- The User does not have sufficient authorizations to carry out the Transaction, or the authorizations are unclear;
- The User's need to carry out the Transaction has not been reasonably justified;
- The User is a fictitious person;
- The User or the representative of the User refuses to provide information for the purposes of establishing the substance of the Transactions and assessment of the risks;
- The User has not presented sufficient data or documents to prove the 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 User, the Beneficial Owner of a User, or another person associated with the User (e.g. director, representative) is or has been linked with organized crime, ML or TF, tax evasion, bribery or corruption;

- The User, the Beneficial Owner of a User, or another person associated with the User 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 User, the Representative or the Beneficial Owner;
- The User advocates, promotes, or assists any violence or any unlawful act.

9. Storage of data

9.1. 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.

9.2. 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 expiration of the Business Relationship or completion of the transaction.

10. Suspicious transaction report

10.1. 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 be promptly escalated to the MLRO.

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

11. Implementation of International Sanctions:

11.1. The Company conducts inspections and pays special attention to all its Users (existing and new) on their activities, as well as to facts and indicators that indicate the possibility that the User is the subject of existing international sanctions.

12. Restricted jurisdictions

12.1. 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 Congo), Guinea-Bissau, Liberia, Libya, Mali, Sierra Leone, Somalia, Cote d'Ivoire, the United States of America (USA), Zimbabwe, Puerto Rico, the United States Virgin Islands, any other possessions of the United States of America or countries in the territory where transactions with digital assets are prohibited or in any way restricted.

12.2. Restriction for Users from the USA.

The user confirms that he is not a US citizen, does not have a permanent residence permit (residence permit) in the USA, is not a US tax resident in accordance with US law, and has not been in the territory of this state for at least the period established by the legislation of a foreign state for recognition as a US tax resident, the country of registration/the establishment of the legal entity – User is not the territory of the United States.

Otherwise, the User undertakes to immediately stop using the Site and Services.

12.3. Prohibition on the sale of Services.
The company does not serve Users who are prohibited by their local law from interacting with cryptocurrency.
Countries where individuals are prohibited from owning, using and disposing of cryptocurrency under the threat of personal criminal liability: Iraq, China, Algeria, Bangladesh, Egypt, Afghanistan.

12.4. The Company 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 resident of 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, Services reserves the right to take any appropriate actions with compliance to the local jurisdiction, including termination of your access to the Services.

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