J’JO AML Policy

Effective date: 11.02.2021

J’JO Anti-Money Laundering Policy (hereinafter - the “**Policy**”) is designated to prevent and mitigate possible risks of J’JO being involved in any kind of illegal activity.
In this Policy, “**we**”, “**us**”, “**our**” and “**J’JO**” refer to JJO OÜ - a company incorporated under the laws of the Republic of Estonia under registration number 14731894. The company’s registered office is at Harju maakond, Tallinn, Kesklinna linnaosa, Roseni tn 13, 10111.

J’JO pays thorough attention to any activities that may be considered as money laundering or terrorist financing. J’JO AML policy is designed to prevent money laundering by complying with AML legislation obligations including the need to have adequate systems and controls in place to mitigate the risk of being used to facilitate the financial crime. To minimize and mitigate the risk of money laundering and/or terrorist financing, J’JO implemented effective internal measures and procedures:

- Establishment of the identity of J’JO Users;
- Assessment of risk;
- Monitoring of transactions; and
- Reporting of suspicious activities to respective authorities.

1. LEGISLATIVE BASIS

Money laundering is a criminal process involving the conversion of the amount of illegally obtained funds (terrorism, corruption, drug trafficking, etc.) while hiding the true source in legal investments. This is because the illegal nature of such funds will not be detected because of their material values.
The country's government is fighting money laundering and terrorist financial transactions in connection with the need to prevent criminal funds from entering the economy. Financial and commercial institutions are most accessible to illegal processes of terrorist and criminal organizations. Digital currency services are particularly vulnerable.

This document and all underlying policies, processes and procedures are prepared in line with provisions, requirements and recommendations of:

1. Money Laundering and Terrorist Financing Prevention Act of Estonia, as amended from time to time ("Act");
2. International Sanctions Act of Estonia as amended from time to time;
3. Directive 2015/849 of the European Parliament and of The Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing” and
4. FATF Guidance for a Risk-Based Approach to Virtual Assets and Virtual Assets Service Providers.

As a regulated business, J’JO is required to comply with the Money Laundering and Terrorist Financing Prevention Act and International Sanctions Act, which require J’JO to identify and verify its Users' identities, conduct ongoing monitoring of their activity, including transaction monitoring, maintain records of Users' activity and related documents for at least five years and report certain transactions to authorities.

2. DEFINITIONS

Money laundering is:

- the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person’s action;

- the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity;
- the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity;
- participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions mentioned in the foregoing points.

Terrorism financing is the provision or collection of funds and other assets, by any means, directly or indirectly, with a view to, or in the knowledge that those means will be used in full or in part by a terrorist organization or by a terrorist acting alone, even without any connection to a particular act of terrorism.

3. IDENTIFICATION OF J'JO USERS

User identification and verification (KYC)

The formal identification of Users while using our service for purchase of the cryptocurrency on entry into commercial relations is a vital element for the regulations relating to money laundering. This identification relies on the following fundamental principles:

- Each User (each individual person and/or each person involved in the case of a legal entity) shall be identified by means of supporting documents.
- These documents will be recorded in a centralized system.
- Distance identification is authorized and possible within a dedicated acceptance process.
- A person will not be accepted as a User if the identification process proves to be incomplete.

J'JO's identity verification procedure requires the User to provide J'JO with reliable, independent source documents, data or information. For such purposes J'JO reserves the right to collect User's identification information for the AML purposes.

J'JO will take steps to confirm the authenticity of documents and information provided by the Users. All legal methods for double-checking identification information will be used and J'JO reserves the right to investigate certain Users who have been determined to be risky or suspicious.

J'JO reserves the right to verify User's identity in an on-going basis, especially when their identification information has been changed or their activity seemed to be suspicious (unusual for the particular User). In addition, J'JO reserves the right to request up-to-date documents from the Users, even though they have passed identity verification in the past.

Information about the user's identification will be collected, stored, shared and protected strictly in accordance with the J'JO's Privacy Policy and relevant rules.

Once the User's identity has been verified, J'JO is able to remove itself from potential legal liability in a situation where its services are used to conduct illegal activity.

After confirming the identity of the User, J'JO may refuse to provide services to the User if J'JO's services are used for the purposes of conducting illegal activities.

4. MULTIPLE ACCOUNT POLICY

It is forbidden to have more than one Account on our Website and/or App.

If it is discovered that the User has more than one account, all accounts will be temporarily blocked. The User will be asked to choose which of his accounts will be active, and the rest will remain blocked forever.

If it is discovered that the User creates several accounts in order to overcome the restrictions set by J'JO for a particular payment method, J'JO reserves the right to request additional verification from the User. If the User cannot provide the requested information, J'JO will return the payment to the original sender, while retaining the incoming and outgoing transaction fees, if applicable.

5. ASSESSMENT OF RISK

J'JO, in line with the international requirements, has adopted a risk-based approach to combating money laundering and terrorist financing. By adopting a risk-based approach, J'JO is able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate to the identified risks. This will allow resources to be allocated in the most efficient ways. The principle is that resources should be directed in accordance with priorities so that the greatest risks receive the highest attention.

6. MONITORING OF TRANSACTIONS

The Users are known not only by verifying their identity (who they are) but, more importantly, by analyzing their transactional patterns (what they do). Therefore, J'JO relies on data analysis as a risk-assessment and suspicion detection tool. J'JO performs a variety of compliance-related tasks, including capturing data, filtering, record-keeping, investigation management, and reporting.

System functionalities include:
1) Daily check of Users against recognized "blacklists", aggregating transfers by multiple data points, placing Users on watch and service denial lists, opening cases for investigation where needed, sending internal communications and filling out statutory reports, if applicable;
2) Case and document management.

With regard to the Policy, J'JO will monitor all transactions and it reserves the right to:

- ensure that transactions of suspicious nature are reported to the proper law enforcement through the Compliance Officer;
- request the User to provide any additional information and documents in case of suspicious transactions;
- suspend or terminate User Account when J'JO has reasonably suspicion that such User engaged in illegal activity.

The above list is not exhaustive, and the Compliance Officer will monitor Users' transactions on a day-to-day basis in order to define whether such transactions are to be reported and treated as suspicious or are to be treated as bona fide.

7. REPORTING TO THE AUTHORITIES

Following its Policy and the applicable legal acts, J'JO, when necessary, will report to the respective authorities of the activities that may be considered as money laundering and terrorist financing. J'JO will not disclose any information about such report to have been made and will not address any questions in relation to that.

8. COMPLIANCE OFFICER

The management board of the J'JO appointed a Compliance Officer, who performs AML duties and obligations of the J'JO. A Compliance Officer reports directly to the management board and has the competence, means and access to relevant information across all the structural units of the J'JO.
Only a person who has the education, professional suitability, the abilities, personal qualities, experience and impeccable reputation required for performance of the duties listed below may be appointed as a Compliance Officer.
The duties of a Compliance Officer include, inter alia:

- organization of the collection and analysis of information referring to unusual transactions or transactions or circumstances suspected of money laundering or terrorist financing, which have become evident in the activities of the J'JO;
- periodic submission of written statements on compliance with the requirements arising from the Act to the management board of the J'JO;
- performance of other duties and obligations related to compliance with the requirements of the Act.

9. COMPLIANCE TRAINING

All J'JO employees and officers receive ongoing broad-based AML training, as well as position-specific training. Training must be repeated at least once every twelve (12) months to ensure employees remain knowledgeable and in compliance with all pertinent laws and regulations. New employees receive training within thirty (30) days of their start date. All documentation related to compliance training including materials, tests, results, attendance and date of completion are maintained. In addition, the J'JO compliance training program is updated as necessary to reflect current laws and regulations.

10. CONTACT US

If you have any questions about this Policy, you can either:

E-mail us: support@jjoapp.io

Write to us: Harju maakond, Tallinn, Kesklinna linnaosa, Roseni tn 13, 10111