FNK Technical Ltd Anti-Money Laundering Policy

1. Introduction.

FNK Technical Ltd (hereinafter – the «Service provider», «FNK») Anti-Money Laundering Policy (hereinafter – the «AML Policy») is designated to prevent and mitigate possible risks of FNK being involved in any kind of illegal activity.

International and Republic of Marshall Islands legislation require Service Provider to implement effective internal procedures and mechanisms to prevent money laundering and to take action in case of any form of suspicious activity from its Users.

This practical instruction sets out internal security measures Employees of the Service Provider and its business partners must know and strictly comply with the requirements set out in the Law of Anti-Money Laundering and Terrorist Financing; in the Anti-Money Laundering instructions, issued for detecting signs of a transaction with suspected money laundering and terrorist financing, as well as for detecting unusual transactions.

2. General definitions.

Cryptocurrency – property value concentrated within a digital unit that can usually be obtained by converting an officially recognised currency and at the same time selling a Cryptocurrency in exchange for an officially recognised currency.

Website –https://fnk.com.

User – any user of the website https://fnk.com.

AML – set of internal rules and measures imposed upon the employees of FNK with the purpose of abiding to and/or being compliant with applicable laws on the prevention of money laundering and terrorist financing.

Service provider – legal entity being a service provider that, in the course of its economic activity, allows the client to make the virtual currency exchange for money and use the wallet service for virtual currency for fee (service charge) based on terms of Transaction concluded between the Service provider and the Client.

Client – capable physical person and/or a legal entity with which the Service provider maintains business relations and whose identity is ascertained as per the identity paper prior to sign a transaction between the Service provider or the partner of the Service provider in line with requirements of the AML, internal procedural rules of the corporate Commercial Association and its bylaws.

Employee – Service provider whose task is to build and maintain business relations, to process data relating to transactions, to identify and assess risks, and to minimize and manage risks.

Politically exposed person (hereinafter – the «**PEP**») – refers to individuals who are or have been entrusted with prominent public functions, their immediate family members or persons known to be close associates of such persons but shall not include middle ranking or more junior officials.

3. General information.

AML Policy covers the following matters:

1. Verification procedures.
2. Monitoring Transactions.
3. Risk Assessment.

4. Verification procedures.

Customer Due Diligence ("CDD") is one of the main international standards for preventing illegal activity. Under the CDD, FNK establishes its own verification procedures as part of its anti-money laundering standards.

FNK's identity verification procedures require the User to provide FNK with reliable, source-independent documents, data or information:

1) first and last name;

2) date and place of birth;

3) the type and number of the document used for identification and verification of identity, the date of issue and the name of the issuing authority;

4) the person's residence address and his/her specialty or field of activity

5) the purpose of the operation and the date of performance thereof;

6) if the client is a natural person from another state party to the European Economic Area Agreement or from a third country, the employee shall register the information on whether this person performs significant tasks of the public authority, is a close employee or a family member of the performer of significant tasks of the public authority.

The following documents may be used as a basis for identifying an individual:

(1) Documents issued under the laws of the Republic of the Marshall Islands: identification card; electronic identification card; residence card; Marshall Islands passport; diplomatic passport; seaman's service book; alien passport; temporary travel document; refugee travel document; naval certificate; repatriation certificate; repatriation permit;

2) a valid travel document or driver's license issued by a foreign country, if the document includes the User's name, photo or image of the person, signature For these purposes, FNK reserves the right to collect the User's identification information for AML/CFT policy purposes.

FNK will take steps to verify the authenticity of documents and information provided by Users. All lawful methods of cross-checking identity information will be used and FNK reserves the right to investigate certain Users who have been identified as risky or suspicious.

FNK reserves the right to verify the identity of Users on an ongoing basis, especially if their identity information has been changed or their activity appears suspicious (unusual for that User). In addition, FNK reserves the right to ask Users for up-to-date documents, even if they have already undergone identity checks in the past.

The collection, storage, transfer and protection of the User's identification information will be strictly in accordance with FNK's Privacy Policy and the relevant regulations.

After verifying the User's identity, FNK may indemnify itself from potential legal liability in a situation where its Services are used to carry out illegal activities.

Users who intend to use payment cards in connection with the FNK Services must have their card verified.

5. Monitoring Transactions.

Users are known not only by verifying their identity (who they are), but more importantly, by analyzing their transactional patterns (what they do). Therefore, FNK relies on data analysis as a tool to assess risk and identify suspicions. FNK performs a range of compliance-related tasks, including data collection, filtering, record-keeping, investigation management and reporting. System functionality includes:

1) Daily screening of users against recognized blacklists, aggregating transfers across multiple data points, placing users on watch and debarment lists, opening cases for investigation when necessary, sending internal reports and completing statutory reports as applicable;

2) Case and document management.

With respect to AML policy, FNK will monitor all transactions and reserves the right to:

1. ensure that transactions of a suspicious nature are reported to the proper law;

2. request any additional information and documents from the User in case of suspicious transactions;

3. suspend or terminate a User's account if FNK has reasonable suspicion that such User is engaging in illegal activity.

The above list is not exhaustive and FNK will monitor Users' transactions on a daily basis to determine whether such transactions should be reported and treated as suspicious or should be treated as *bona fide*.

A Service Provider employee is prohibited from transacting:

1. With a person who refuses to provide data;
2. If the customer fails to provide the necessary documents and relevant data;
3. If, on the basis of the submitted documents, the employee suspects that money laundering or terrorist financing may be involved;
4. If the person on whose behalf or for whose account another person is acting is not identifiable or is suspected to be a front man.

6. Risk Assessment.

FNK, in accordance with international requirements, has adopted a risk-based approach to combating money laundering and terrorist financing. By adopting a risk-based approach, FNK can ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. This will allow resources to be allocated in the most efficient way possible. The principle is that resources should be prioritized so that the greatest risks receive the most attention.

When assessing money laundering and terrorist financing risk, the service provider should consider three categories of risk: geographic risk, customer risk, and transaction risk.

Geographic risk is considered high if the customer is known to be from the following countries:

1. countries and territories subject to United Nations ("UN") or European Union ("EU") sanctions, embargoes or other similar measures; countries and territories subject to sanctions, embargoes or other similar measures "EU");

2. countries which do not apply adequate measures to combat money laundering and terrorist financing as determined by the Financial Action Task Force (FATF) or the European Union

3. countries reliably associated with supporters of terrorism or countries with high levels of corruption.

A customer's risk is considered high if the customer:

1. is such a person or his or her relationship with others is so confusing or unusual that the actual beneficiary cannot be identified;

2. is a PEP;

3. Is on the UN or EU list of persons subject to international financial sanctions (published on the Money Laundering Compliance Division's website);

4. is a person previously suspected of probable connection with money laundering or terrorist financing.

5. the behavior, appearance and transaction amount of the customer is suspicious.

The following factors indicate a suspicious person:

1) the person's appearance and conduct do not match the nature of the transaction he or she is making, or the person's conduct does not inspire confidence;

2) the person turns to third persons for help in filling out the documents or does not know how to fill them out;

3) the person's representative attempts to conceal the actual client or does not know the client's data

4) the person attempts to conclude a sham or other illegal transaction;

5) the person is suspected of carrying out the transaction on behalf of and at the expense of another person

6) it is known that the person is involved in money laundering.

The risk associated with a transaction is considered high if:

1) the value of the transaction exceeds 15,000 euros or the equivalent amount in another currency;

2) a third party pays for the transaction in cash, not being a party to the transaction.

7. Governing Law & Jurisdiction.

This Agreement shall be governed by and construed in accordance with the laws of Republic of Marshall Islands.

The parties agree to irrevocably submit to the exclusive jurisdiction of the courts in Republic of Marshall Islands for the resolution of any disputes arising from this AML Policy or in connection therewith or pursuant thereto.

8. Modifications.

These rules may be periodically reviewed and revised. The revised rules will be uploaded on the FNK Website and will reflect the modified date of the rules. The User is required to periodically visit the Website and review the rules and any changes thereto.

Continued use of the FNK Website constitutes the agreement of User to the rules contained herein and any amendments thereto.