MAINSTON INTERNATIONAL OÜ

RISK ASSESSMENT 2022

Approved by the Management Board of MAINSTON INTERNATIONAL OÜ on 01.06.2022

1. Risk assessment basis and renewal process

1.1. Risk assessment is based on the Law on the Prevention of Money Laundering and Terrorist Financing, the Financial Intelligence Unit's guidelines, common guidelines prepared on the basis of Articles 17 and 18 (4) of EU Directive 2015/849, the Estonian National Money Laundering and Terrorist Financing Risk Assessment 2020 and the guidelines of International organizations.

1.2. In compiling the risk assessment, MAINSTON INTERNATIONAL OÜ maps the risks related to money laundering and terrorist financing related to its operations, then assesses the effects of the mapped risks on the operations of MAINSTON INTERNATIONAL OÜ and analyzes possible countermeasures that can be used to mitigate the risks.

1.3. MAINSTON INTERNATIONAL OÜ documents the risk assessment and risk appetite identification and updates these documents as necessary, but at least once a year and according to the result of the national risk assessment.

1.4. As a result of the risk assessment, MAINSTON INTERNATIONAL OÜ identifies:

1.4.1. Areas with a lower and higher risk of money laundering and terrorist financing;

1.4.2. Risk appetite, including the volume and extent of products and services offered in the course of business;

1.4.3. A risk management model to mitigate the identified risks.

1.5. The identification of risk appetite takes into account the risks that MAINSTON INTERNATIONAL OÜ is willing to take or wants to avoid in connection with its business activities and qualitative and

quantitative compensation mechanisms, such as planned income, capital or other liquidity measures or other circumstances such as reputational risks and money laundering and legal and other risks associated with terrorist financing or other unethical practices.

2. Risk Appetite

2.1.In order to avoid risks that MAINSTON INTERNATIONAL OÜ is not ready to take in its business operations, risk factors and characteristics have been identified, the occurrence of which in a risk profiled person prohibit entering into a business relationship:

2.1.1. with persons for whom due diligence measures cannot be performed;

2.1.2. persons with whom money laundering and/or terrorist financing is known or suspected in the course of due diligence measures;

2.1.3. anonymous and/or fictitious persons and straw men;

2.1.4. shell banks and such credit institutions or financial institutions that knowingly allow shell banks use their accounts (no correspondent relationship is established);

2.1.5. persons who are included in the UN, OFAC and EU lists of sanctions;

2.1.6. natural or legal persons who are from high-risk FATF countries (with insufficient measures for prevention of money laundering and terrorist financing);

2.1.7. providers of tumbler/mixer services;

2.1.8. persons whose bearer shares or other bearer securities represent more than 10 per cent of the capital;

3. Background Overview of the Company and its Services

3.1. The Company is registered in Estonia with the registration number 14763925, registered address at Viru väljak 2 Kesklinna linnaosa, Tallinn Harju maakond 10111.

3.2. The Company is a virtual currency service provider with an activity license No FVT000240 issued in accordance with Section 70 of the AML Act.

3.3. The business of the Company consists of the provision of virtual currency exchange and wallet service, whereby Clients can deposit and exchange virtual currencies on the Company's website: https://mainston.com/

3.4. The Company will use third party Service Providers, either specialized service providers or who are licensed themselves under AML Act, to provide client identification and verification services. Management of ML/TF related risks, including designing Company´s risk management model, risk appetite, procedures, appropriate organization and stuffing is done by the Company itself.

3.5. For Client identification and verification, as well as for PEP and Sanctions check, the Company is using the services of Onfido SAS, Shufti Pro Limited.

3.6. For transaction monitoring, the company is using the services of Tangany GmbH.

3.7. For blockchain monitoring, the company is using Qlue

4. General risk assessment on the business model of the Company

4.1. Taken into account the business model of the Company and given the nature of its activities, the Company is exposed to a considerable amount of risks of ML/TF.

4.2. Based on the Company´s business model the Company enables Clients to deposit, exchange and buy virtual currencies on the Company's App: The Clients can also store their virtual currencies in a digital wallet provided by the Company and transfer virtual currencies to and from that digital wallet from digital wallets with other service providers.

4.3. In case, if the company will decide to receive the fiat, the Company could receive payments in fiat currency from Client only via authorised payment service providers (payment accounts and credit card providers) happens via the same payment service provider, or the company will accept the fiat deposits only from the sepa transfers from the wallet holders accounts. On the other hand, once the fiat is exchanged into virtual currency, the transfer to another digital wallet is not subject to similar regulations. Therefore, the Company´s business model involves ML/TF risks that are usual for the virtual currency service providers enabling its Clients to pay and transact with virtual currencies.

4.4. The role of the Company is limited to controlling the funds received and exchanging the fiat to virtual currency based on the specific instructions received from the Client.

4.5. The Company mitigates the ML/TF risks by requiring each Client to be identified and the identity to be verified in accordance with the AML Act by using the means of technological solutions provided the external Service Providers. This allows the Company to increase confidence that any fraudulent activities are caught.

4.6. Risk classification

4.6.1. At least the following risk categories shall be taken into account when preparing the risk assessment and identifying customer risk profile:

1) Risk associated with the customer;
2) Risk associated with countries or geographical areas or jurisdictions;
3) Risk associated with the products, services or transactions;
4) Risk associated with the communication or mediation channels between MAINSTON INTERNATIONAL OÜ and the customer or the transmission channels of products, services or transactions.

5. Approval matrix

Client Risk Score	AML/KYC Specialist	Compliance Officer	Board of Directors
High		✓	
Medium	✓		
Low	✓		
PEPs			✓

6. Customer risk

6.1. Where the risk factors arise from the person who is a party to a transaction or the person of a customer:

6.1.1. the person´s residency;

6.1.2. whether it is easy to establish the origin of the person's wealth or the source and origin of the funds used for a transaction;

6.1.3. whether there is any negative media information on the person;

6.1.4. the customer's legal form, management structure, including whether the customer is a trust fund, civil law partnership or other such contractual legal entity;

6.1.5. whether it is complicated to determine the person's beneficial owners due to complicated and non-transparent owner relations;

6.1.6. duration of business operation and experience.

6.1.7. whether the customer is as PEP.

6.1.8. whether the customer is subject to sanctions.

6.1.9. whether the customer is involved with cash-intensive business

6.2. Customer risk increasing circumstances are:

6.2.1. Business relationship foundations based on unusual factors or there are unusual transactions patterns without clear economic or lawful purpose

6.2.2. Customer is a resident of a higher-risk geographic area

6.2.3. Customer or its affiliate has nominee shareholders or bearer shares

6.2.4. Unusual or complex ownership structure

6.3. How Mainston OÜ is mitigating the Customer risk:

6.3.1. Mainston OÜ has implemented the requirements from the Estonian AML Act in its internal AML/CTF procedures.

6.3.2. Mainston OÜ is using well known IT systems and KYC service providers mentioned in sections 3.5-3.7 in order to ensure the identification and background check of every customer.

6.3.3. Mainston OÜ is conducting random checks on the service providers in order to ensure that all the lists are up to date.

6.3.4. Not accepting the persons with unusual or unreasonably complex ownership structure if it makes impossible to identify beneficial owners of the Client.

6.3.5. Not accepting PEPs as Client

6.4. General Customer risk mitigating circumstances:

6.4.1. Customer is a company listed on a regulated market, which is subject to disclosure obligations that establish requirements for ensuring sufficient transparency regarding the beneficial owner

6.4.2. the customer is an institution of the European Union

6.4.3. Customer is a person who is a resident of EEA

7. Geographical risk

7.1. Geographical risk or the risk arising from the differences in the legal environment in different countries, with which the Customer or the Customer´s representative or the actual beneficiary is related, including:

7.1.1. whether the country implements legal norms in accordance with international standards for the prevention of money laundering and terrorist financing;

7.1.2. whether the country has a high crime level, including drug related crime level;

7.1.3. whether the country is cooperating with a criminal organization; whether criminal organizations use the specific country to carry out their own activities;

7.1.4. whether the country is engaged in financing the proliferation of weapons of mass destruction;

7.1.5. whether the country has a high level of corruption;

7.1.6. whether international sanctions have been or are being applied to the country;

7.1.7. whether other measures have been applied to the country or the views of international organizations towards the country have been published.

7.2. Geographical risk increasing circumstances are, in particular, situations in which the person involved in the transaction or the transaction itself is linked to a country or jurisdiction:

7.2.1. where, according to reliable sources, such as peer reviews, detailed evaluation reports or published ex-post reports, effective systems for preventing money laundering and terrorist financing are not in place;

7.2.2. where, according to reliable sources, the level of corruption or other criminal activity is significant;

7.2.3. which is a subject to sanctions, embargoes or similar measures, such as those imposed by the European Union or the United Nations;

7.2.4. which finances or supports terrorism or on whose territory organizations, that are designated by the European Union or the United Nations, operate.

7.3. Geographical risk mitigating circumstances are, in particular, situations where the party or the transaction originates from or resides in the following country:

7.3.1. in a Contracting State of the European Economic Area;

7.3.2. in a third country with effective systems to prevent money laundering and terrorist financing;

7.3.3. in a third country where, according to reliable sources, the level of corruption and other criminal activity is low;

7.3.4. in a third country where, according to reliable sources, such as peer reviews, reports or follow-up reports, anti-money laundering and anti-terrorist financing requirements are in place and in line with the revised recommendations of the Anti Money Laundering Board and are effective

7.4.

Country	**Decision**	**Risk Parameter**	**Result**
European Union, Switzerland	Low		SDD measures as per the AML Manual can be applied.
The rest of the world	Medium		CDD measures as per the AML Manual will be applied.
Russia (countries under the international sanctions)	High		Entire application will be risk rated as High. EDD measures as per the AML Manual will be applied.
Afghanistan Bosnia & Herzegovina	Prohibited		Application will be rejected.

Cambodgia Dempcratic People's Republic of Korea Ethiopia Ghana Guyana Iceland Iran Iraq Laos Mongolia North Macedonia Pakistan Panama Sri Lanka Syria Trinidad and Tobago Tunisia Uganda United States Vanuatu Yemen			

8. Risk associated with the products, services or transactions

8.1. Products or services risk is where the risk factors arise from the customer's economic operation and exposure of the specific product or service to potential money laundering risks:

8.1.1. customer buys virtual currency with cash;

8.1.2. customer has more than 3 wallet accounts;

8.1.3. virtual currency exchanged by the customer has transferred through the dark web or the use of a mixer/tumbler service is suspected;

8.1.4. the origin of the virtual currency or customer´s funds is not easily established.

8.2. Product or service risk increasing circumstances are, in particular, situations involving:

8.2.1. Entering into or arranging a transaction that may promote anonymity;

8.2.2. Payments received from unknown or unrelated third parties;

8.2.3. A business relationship or a transaction that is established or initiated in a manner in which the Customer, its representative or a party to the transaction is not present in the same place and the identity is not verified by means of information technology;

8.2.4. New products or new business practices, including the use of a new transmission mechanism or new or evolving technology for both new and existing products.

8.3. Product or service risk mitigating circumstances are, in particular, situations where:

8.3.1. Financial products or services that provide appropriately identified and limited services to specific customer groups in order to increase the availability of financial services;

8.3.2. Products for which the risk of money laundering and terrorist financing is managed by other factors, such as monetary thresholds.

8.4. Risk related to exchange of tokens. Limited exchange only (STON to USDT).

8.4.1. Classical risks related to exchange operations - use of false identity, trade with assets having unidentified origin and history.

8.4.2. To mitigate risk related to exchange of tokens Mainston OÜ has limited exchange services to the maximum extent, excluding exchange using fiat and cash. Each and every customer is identified, incl. proof of address. In cases of operation with substantial funds (exceeding limits set by Mainston) as well as using company identity, Tier 3 and 4 of onboarding measures are rehearsed.

8.5. Risk related to wallet service

8.5.1. Classical virtual currency service risks - False identity and address, false IP.

8.5.2. To mitigate risk related to wallet service Mainston OÜ is implementing Tier 1, 2, 3, 4 KYC policy which reduce risks to a minimum as each and every customer is identified on a documentary basis and address proofed to exclude country, territory, PEP and sanctions risks.

9. Communication channel risk

9.1. Communication channel risk, the risk factors of which arise from the use of different communication channels:

9.1.1. whether a previously used IP address or a new IP address is used when logging in to the web platform;

9.1.2. whether it is a new customer or a customer who has already used the service;

9.1.3. whether the customer can be identified and verified through real-time surveys using a synchronized audio and video stream;

9.1.4. whether the submitted data, IDs and other documents can be verified using a reliable and independent source;

9.1.5. whether the IP address from which the customer starts transactions differs from the country where the customer / customer´s representative resides;

9.1.6. whether the customer / customer´s representative uses a telephone number different from the one in the country of residence.

9.2. How Mainston OÜ is mitigating the communication channel risk:

9.2.1. Mainston OÜ has implemented the requirements from the Estonian AML Act in its internal AML/CTF procedures.

9.2.2. Mainston OÜ is using well known IT systems and service providers mentioned in sections 3.5-3.7 for identification, verification and transaction monitoring.

9.2.3. Mainston OÜ is conducting random checks on the service providers in order to ensure that all the lists are up to date.

10. Measures to mitigate the risks associated with virtual currency exchange services

10.1. mobile phone number and e-mail address is collected from the customer, the validity of which is checked once every six months (by sending control codes);

10.2. service delivery risks are mitigated by performing automatic check and internal control activities to continuously assess the system´s ability to detect unusual or suspicious transactions, changes in sanction lists, the volume and quality provided by customers etc;

10.3. An approved service provider is used to identify the customer´s wallet address and to monitor virtual currency transactions;

10.4.the monitoring program is structured in a way that it detects the overlap of the counterparty with a politically exposed persons and persons/companies on the sanctions lists;

10.5. the monitoring program is structured in a way that it identifies the possession of multiple wallets and related transactions by a single customer;

10.6.the monitoring program is structured in a way that it can detect suspicious and unusual transactions;

10.7.where appropriate, the source and origin of funds used in a transaction can be verified;

10.8. all customers who are using the online platform are identified by comparing an identity document with a so-called profile photo (selfie).

11. Client risk level

11.1. Assigning a risk level to the customer must be documented and risk level must be updated if necessary during the business relationship. The risk factor assessment must ensure that:

- the risk assessment is not unduly affected only by a single risk factor;
- the risk assessment is not affected by economic or profit related considerations.

11.1.1. Based on the data collected in the course of customer identification, the CRM program used by MAINSTON INTERNATIONAL OÜ assigns a risk level to each customer, according to the score obtained in the assessment of risk categories and risk factors.

11.1.2. The risk levels are low, medium and high. The basic parameters used by the CRM program to determine the risk level are following:

11.1.2.1. Customer´s place of residence or place of business and the place of residence of the beneficial owner (geographical risk);

11.1.2.2. Special characteristics that shape the risk profile (PEP status, negative media, etc.);

11.1.2.3. Economic activity (estimated monthly turnover, activities and experience in the given industry, operating in an industry that trades in new and/or evolving technologies and/or transmits its services through non-traditional sales channels);

11.1.2.4. Counterparties and their related risks (including operating in an industry that trades in new and/or evolving technologies and/or communicates its services through nontraditional sales channels).

11.2 Low risk characteristics

11.2.1. There is no influential risk factor in any of the higher risk categories and at least one risk mitigating factor exists, therefore, it can be stated that the Customer and his/her activities correspond to characteristics that are not different from those of a person with normal and transparent activities, thereby there is no doubt that the Customer´s activities may increase the probability of money laundering and terrorist financing;

11.2.2. The Customer and its transaction partners are located in EU or EEA countries;

11.2.3. information about the Customer and his/her actual beneficiary is publicly available, the person´s activities and transactions are in accordance with his/her daily business activities and do not differ from the payment behavior of other similar Customers or where there are quantitative or other absolute restrictions on the provision of the transaction.

11.2.4. the customer pays for the virtual currency through a payment account located in a credit institution, electronic money institution or a payment institution which is established or provides services in an EU or EEA country.

11.2.5. the virtual currency wallet is used to store virtual currencies purchased only from MAINSTON INTERNATIONAL OÜ and no transfers of virtual currencies to and from third parties are made;

11.2.6. the customer and/or its counterparties are located in third countries with effective anti-money laundering and anti-terrorist financing systems.

11.3. Medium risk characteristics

11.3.1. the customer pays for the virtual currency through a payment account located in a credit institution, electronic money institution or payment institution which is established outside a contracting state of the European Economic Area;

11.3.2. the customer makes transfers of virtual currencies to virtual currency wallets that are opened in a financial institution that is not subjected to requirements equivalent to RahaPTS.

11.4. High risk characteristics

11.4.1. The Customer´s risk level is generally high if, when assessing the risk categories as a whole, a suspicion arises that the Customer´s activities are not normal or transparent, ie at least one of the higher

risk categories exists, which may lead to a high or significantly increased probability of money laundering and terrorist financing. Customer´s risk level is also high if it is expected by any of the risk factor indicators (e.g. suspicion of being the subject of an international sanction). However, high risk level does not necessarily mean that the Customer is engaged in money laundering or terrorist financing.

11.4.2. The risk level is always considered high in the case of a Customer whose representative or beneficial owner is domiciled in a high-risk third country or territory where adequate measures to prevent money laundering and terrorist financing have not been implemented or if that country or territory does not cooperate internationally in the prevention of money laundering or terrorist financing or is a low-tax territory.

11.4.3. The risk level is always considered high if the circumstances of the transaction indicate money laundering and terrorist financing or are likely to be linked to money laundering and terrorist financing, including in the case of complex, high-value and unusual transactions that do not have a reasonable economic purpose.

11.4.4. If a MAINSTON INTERNATIONAL OÜ employee considers the risk level of a Customer or a person participating in the transaction to be high, then the employee must apply enhanced due diligence measures.

12. Identification of risks associated with new and existing technologies, products and services.

12.1. Before offering a new financial service or product or new or non-traditional sales channels to Customers or introducing new or evolving technologies, the Management Board of MAINSTON INTERNATIONAL OÜ , in cooperation with the FIU contact person (AML compliance officer), assesses the risks of money laundering and terrorist financing associated with the products or services.

12.2. In order to assess the risks, the Management Board of MAINSTON INTERNATIONAL OÜ , together with the appointed FIU contact person (AML compliance officer) and, if necessary, other employees, maps the risks associated with each new product service, technology or sales channel.

12.3. The risk assessment assesses both actual and potential risks and, if necessary, collects additional information on the risks and risk mitigation measures.

12.4. After mapping out the risks, the Management Board of MAINSTON INTERNATIONAL OÜ assesses the probability of risk realization and risk level, paying special attention to the circumstances that increase and decrease the risks.

12.5. After assessing the risks and their effects, MAINSTON INTERNATIONAL OÜ assesses the most appropriate countermeasures to mitigate specific risks to the level corresponding to the MAINSTON INTERNATIONAL OÜ ´s Risk Appetite and, if necessary, organizes the application of the respective measures.

12.6. MAINSTON INTERNATIONAL OÜ assesses whether the application of measures can bring the risks of money laundering and terrorist financing associated with new financial services or products, new or non-traditional sales channels or new or evolving technologies to a level that meets the MAINSTON INTERNATIONAL OÜ ´s Risk Appetite risk levels.

12.7. Offering a new financial service or product, new or non-traditional sales channels to the Customer or introducing a new or evolving technology may only be started if the associated money laundering and terrorist financing risks are in line with MAINSTON INTERNATIONAL OÜ ´s Risk Appetite or those risk can be brought to an acceptable level.

13. Risk Management Model

13.1. MAINSTON INTERNATIONAL OÜ ´s Management Board takes into account the risks and risk appetite presented in this Risk Assessment when making decisions concerning the general management of the company (preparation of business strategy, development of new products/services). Proportionate and risk-based application of due diligence measures is a key to mitigate the risks of money laundering and terrorist financing.

13.2. Transmission of information between the management board and the employees

13.2.1. the volumes of risk appetite are monitored by a member of the board on a daily basis.

13.2.2. the FIU contact person (AML compliance officer) reports on the realization/prevention of risks to the Management Board once a year.

13.2.3. employees shall inform the FIU contact person (AML compliance officer) or the responsible member of the Management Board of the identification of the risks related to the activities, products and processes under their responsibility, including the identification of errors in work instructions and/or the program.

13.2.4. in the event of a change in the Risk Appetite or the Risk Assessment, the Management Board shall immediately inform the employees of the changes and make them available electronically.

13.2.5. it is ensured that employees who report a suspicion of money laundering or terrorist financing or a breach of the RahaPTS to the FIU contact person (AML compliance officer) within MAINSTON INTERNATIONAL OÜ, are protected from threats or hostile actions from other employees, members of the management board or customer, and from unfavorable and discriminatory professional treatment.

13.3. to prevent risks, the Management Board:

13.3.1. constantly improves and modernizes the existing IT solutions,

13.3.2. incorporates new, fully automated software solutions to bring the possibility of human error or intentional irregularities to near zero,

13.3.3. takes into account the Rik Appetite when developing new services and, if necessary, carries out additional Risk Assessments,

13.3.4. provides prompt guidance to employees,

13.3.5. ensures effective internal control over the work of the employees by appointing internal auditor