

GENERAL AML/KYC POLICY

1. This Anti-Money Laundering and Know Your Customer Policy (hereinafter - the “AML/KYC Policy”) of **Bizonex OÜ**, (hereinafter “Company”), a company registered in accordance with legislation of Estonia, with registration number 14381075 at Harju maakond, Tallinn, Lasnamäe linnaosa, Narva mnt 150, 13619, reflects main provisions of Company’s compliance policies designated to prevent and mitigate possible risks of the Company being involved in any kind of illegal activity.

2. Both international and local regulations require the Company to implement effective internal procedures and mechanisms to prevent money laundering, terrorist financing, drug and human trafficking, proliferation of weapons of mass destruction, corruption and bribery and to take action in case of any form of suspicious activity from its Users.

VERIFICATION PROCEDURES

3. One of the international standards for preventing illegal activity is customer due diligence (“CDD”). According to CDD, the Company establishes its own verification procedures within the standards of anti-money laundering and “Know Your Customer” frameworks.

4. Company’s identity verification procedure requires the User to provide the Company with reliable, independent source documents, data or information (e.g., national ID, international passport, bank statement, utility bill). For such purposes the Company reserves the right to collect User’s identification information for the AML/KYC Policy purposes.

5. The Company 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 the Company reserves the right to investigate certain Users who have been determined to be risky or suspicious.

6. The Company reserves the right to verify User’s identity in an on-going basis, especially when their activity seemed to be suspicious (unusual for the particular User). In addition, the Company reserves the right to request up-to-date documents from the Users, even though they have passed identity verification in the past.

7. User’s identification information will be collected, stored, shared and protected strictly in

accordance with Company's Privacy Policy and related regulations.

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

COMPLIANCE OFFICER

9. The Compliance Officer is the person, duly authorized by the Company, whose duty is to ensure the effective implementation and enforcement of the AML/KYC Policy. It is the Compliance Officer's responsibility to supervise all aspects of the Company's anti-money laundering and counter-terrorist financing activity, including but not limited to:

- a) Collecting Users' identification information.
- b) Establishing and updating internal policies and procedures for the completion, review, submission and retention of all reports and records required under the applicable laws and regulations.
- c) Monitoring transactions and investigating any significant deviations from normal activity.
- d. Implementing a records management system for appropriate storage and retrieval of documents, files, forms and logs.
- e. Updating risk assessment regularly.
- f. Providing law enforcement with information as required under the applicable laws and regulations.

10. The Compliance Officer is entitled to interact with law enforcement, which are involved in prevention of money laundering, terrorist financing and other illegal activity.

ANTI-MONEY LAUNDERING POLICY

11. The Company enforces a strict anti-money laundering policy with zero tolerance for money laundering activities. We define money laundering as any activity that is carried out in an attempt to misrepresent the source of funds actually acquired through illegal processes as funds that were acquired through lawful sources/activities.

12. All Company's affiliates are obligated to comply with this anti-money laundering policy and internal AML Manuals and with all applicable anti-money laundering laws. Failure

to comply can result in severe consequences such as criminal penalties and heavy fines.

13. The Company ensures complete compliance with laws pertaining to anti money laundering through its related policy.

14. The Company implements a range of filtration operations for swift and accurate identification of any financial activities that may constitute or are related to money laundering. This helps ensure a money laundering-free financial operations throughout the Website.

15. All Users acknowledge, undertake and agree to the following terms regarding their use of the Website, opening and maintenance of accounts at Website and for all financial transactions as a Company`s client:

1) The User will comply (throughout the time as an Company`s client) with all relevant statutes pertaining to money laundering and proceeds from criminal activities.

2) The Company operates under certain obligations known as “know-your-client” obligations which grant the Company with the right to implement anti-money laundering procedures to help detect and prevent money laundering activities where money laundering may mean to handle any funds associated with any illegal activity regardless of the location of such activity.

3) The User agrees to lend full cooperation to the Company with respect to anti-money laundering efforts. This involves providing information that the Company requests regarding the client`s business details, account usage, financial transactions etc. to help the Company to perform its duties as dictated by Applicable laws regardless of jurisdiction.

4) The Company reserves the right to delay or stop any funds transfer if there is reason to believe that completing such a transaction may result in the violation of any applicable law or is contrary to acceptable practices.

5) The Company reserves the right to suspend or terminate any account or freeze the funds in an account if there is reason to believe that the account is being used for activities that are deemed unlawful or fraudulent.

6) The Company has the right to use client information for the investigation and/or prevention of fraudulent or otherwise illegal activities.

7) The Company has the right to share client information with:

a) Investigative agencies or any authorized officers who are helping the Company to comply with applicable law, including anti-money laundering laws and know-your-client obligations;

b) Organizations that help the Company to provide the services it offer to its clients;

c) Government, law enforcement agencies and courts;

d) Regulatory bodies and financial institutions.

16. The Company considers the following activities as possible indications of money laundering:

1) The client showing unusual apprehension or reservations about the Company's anti-money laundering policies.

2) The client's interest in conducting financial transactions which are contrary to good business sense or are inconsistent with the client's business policy.

3) The client failing to provide legitimate sources for their funds.

4) The client providing false information regarding the source of their funds.

5) The Company receive any information that the client is connected with any civil or criminal violations.

6) The client seems to be acting as a 'front man' for an unrevealed personality or business, and does not satisfactorily respond to requests for identifying this personality or business.

7) The client not being able to easily describe the nature of his/her industry.

8) The client frequently makes large deposits in cryptocurrency and demands withdrawal in fiat only.

9) The client maintains multiple accounts and conducts an unusually high number of inter-account or 3rd party transactions.

10) The client's previously usually inactive account starts receiving a surge of wire activity.

The above list is by no means an exhaustive list. The Company monitors its client and account activity in light of several other red flags and takes appropriate measures to prevent money laundering.

17. The Company adopt tiers of User`s access to the platform system to ensure stricter anti-money laundering activity. The level of User`s access at the platform depend on stage of KYC procedure that the relevant User comply with. There are following levels:

1. “Bronze” level of access features:

- Depositing of any funds is prohibited
- Withdrawal of any funds is prohibited.
- Trading is prohibited.

1. “Silver” level of access features:

- User is entitled to deposit of any cryptocurrency and fiat.
- User is entitled to output of any cryptocurrency with a limit equivalent to 5 000 EURO (throughout 30 days).
- Withdrawal of fiat money (e.g. Russian rubles, US dollars, Euros) is prohibited.
- Trading between any cryptocurrency pairs with a limit on trade volume equivalent to 5 000 EURO (throughout 30 days).
- Trading between pairs with fiat money (e.g. Russian rubles, US dollars, Euros) is prohibited.

2. “Gold” level of access features:

- User is entitled to output of any cryptocurrency with a limit equivalent to 15 000 EURO (throughout 30 days).
- User is entitled to withdraw of fiat money (e.g. Russian rubles, US dollars, Euros) with a limit of 15,000 EURO (per day) or 50,000 EURO (throughout 30 days). This provision is applicable only after such feature of the Platform will be released.
- Trading between any pairs with a trade limit equivalent to 50 000 EURO (throughout 30 days). This provision is applicable to trading between crypto-fiat pairs only after fiat currency feature will be released on the Platform.

3. “Platinum” level of access features:

- The User is entitled to output of any cryptocurrency without limits.
- The User is entitled to withdraw of fiat money (e.g. Russian rubles, US dollars, euros) with a limit of 500,000 EURO (throughout 30 days). This provision is applicable only after such feature of the Platform will be released.

- Trading between any pairs without trade limits. This provision is applicable to trading between crypto-fiat pairs only after fiat currency feature will be released on the Platform.

KNOW YOUR CUSTOMER (KYC)

18. The User acknowledges that he/she/it has to complete a KYC check before the start using the Website, which must be in form and substance satisfactory to the Company. KYC check is carried out during the registration on the Website by providing necessary information with regard to identification of the User, beneficial owner and origin of the funds, the scope and type of information depending on the type of User.

19. The Company adopt 4 stages of KYC procedure:

19.1. To comply with Bronze KYC stage and receive “Bronze” level of access the User shall fill the full block "User information" -> "Verification" -> "Personal information" on the page "Personal data". The information must be checked by the Company and confirmed as reliable.

19.2. To comply with Silver KYC stage and receive “Silver” level of access User shall fill the block "User information" -> "Verification" -> "Address" and Funds information" on the page "Personal data" and add relevant documents to the block "User information" -> "Verification" -> "Documents" on the page "Personal data" in accordance with section 21, 22. The information must be checked by the Company and confirmed as reliable.

19.3 To comply with Gold KYC stage and receive “Gold” level of access User shall add relevant documents to the block "User information" -> "Verification" -> "Documents" on the page "Personal data" in accordance with section 23 of this AML/KYC Policy. The information must be checked by the Company and confirmed as reliable.

19.4. To comply with Platinum KYC stage and receive “Platinum” level of access User shall add relevant documents to the block "User information" -> "Verification" -> "Documents"-> "Additional documents"on the page "Personal data". Provided however that the User shall provide the Company with legal documents on each transaction that exceed amount of cryptocurrency or fiat equivalent to 15 000 EURO per transaction. Such documents shall be added to the block "User information" -> "Verification" -> "Photos and agreements" on the

page "Personal data". The information must be checked by moderator and confirmed as reliable.

20. The User acknowledges and agrees that level of access shall be changed no earlier than one day after the information or documents are confirmed by the Company. The confirmation of information and documents provided by the User is conducted in accordance with Company's internal policies.

21. Appropriate documents for verifying the identity of User include, but are not limited to, the following:

1) For an individual User: a high resolution scanned copy or photo of pages of a passport or, for citizens of EU, any other national ID, indicating family name and name(s), date and place of birth, passport number, issue and expiry dates, country of issue and User's signature.;

2) For a corporate User: a high-resolution copy of documents showing the existence of the entity, such as Certificate of Incorporation, and, where applicable, Certificate of Change of Name, Certificate of Good Standing, Articles of incorporation, a government issued business license (if applicable), etc.

22. To verify the address the User shall provide, in the same correct name of the client: a high-resolution copy of a utility bill (fixed-line phone, water, electricity) issued within the last 3 months; A copy of a tax or rates bill from a local authority; A copy of a bank statement (for a current account, deposit account or credit card account); A copy of a bank reference letter.

23. To verify the source of income the User shall provide bank account statement, certificate of income of natural person, financial statements or any other document on the Company's discretion.

24. The Company is entitled to request additional documents from Client to conduct enhanced KYC at any KYC stage.

25. The User is obliged to collaborate with regard to the AML/ KYC check and to provide any information and document deemed necessary by the Company.

26. The Company may reject any User in its sole discretion without being obliged to disclose any reason for the rejection.

27. In case the automatic procedures fail, the Company shall contact the User by email or other means to obtain the information and documents needed. In case the User does not provide the documents in the requested form and any other information requested to satisfy the AML/KYC check within 10 (ten) days which are not public holidays in Estonia of the Company's request, the Company may reject the User and the costs for the AML/KYC check will be at the cost of the User. Additionally, the Company has the right to partially or fully withhold the received amounts for any costs or damages incurred by the Company. All kind of remittance fees either for fiat currency or for cryptocurrencies shall be borne by the User.