

Venus Exchange Services

(14732050)

AML POLICY

2020

A. ANTI-MONEY LAUNDERING

This policy is to establish guidelines for Venus Exchange Services OÜ (“Company” or “Exchange”), Estonia FIU License Number FRK001196 & FVR001315, ‘Anti-Money Laundering’ and ‘Know Your Client’ (“KYC”) procedures for new and existing clients.

All of monetary transactions, to the best knowledge of the Company shall be free from any form of money laundering and terrorist activities. The Company operates with integrity and is committed to implementing the measures established. The Client’s failure to comply with the regulations set by the Company would mean termination of the account. If the Client is proven of committing money laundering, he is responsible for any damage or loss which may occur, and the Company is excluded from his fraudulent actions.

In an effort to counter money laundering and other illegal activity, we have decided not to support any cash transactions, regardless of their stated purpose. Our firm has the right to cancel or deny a transaction at any point if there are suspicions regarding its legality.

Legal Framework

Estonian licensed exchange Companies are required to comply with the provisions of the European 5th AML Directive (the “Law” for the purposes of this policy) regarding the prevention of Money Laundering and Terrorist Financing. The main purpose of the Law is to define and criminalize the laundering of proceeds generated from all serious criminal offences aiming at depriving criminals from the profits of their crimes.

In accordance with the Law, Exchanges are obliged to set out policies and procedures for preventing money laundering activities. Those procedures, which are implemented by the Company, as these are requested by the Law, are the following:

- a. Identification and due diligence procedures of clients.
- b. Record keeping procedures in relation to clients’ identity and their transactions.
- c. Internal reporting procedures to a competent person (e.g. Anti-Money Laundering Compliance Officer) appointed to receive and consider information that give rise to knowledge or suspicion that a client is engaged in money laundering activities.
- d. Appropriate procedures of internal control, risk management, with the purpose of preventing money laundering activities.

- e. The detailed examination of every transaction that due to its nature is considered vulnerable to money laundering, and especially for complicated or unusually large transactions and transactions that are taken place without an obvious financial or legal purpose.
- f. Measures for making employees aware of the above-mentioned procedures to prevent money laundering and of the legislation relating to money laundering.
- g. Provision of regular training to their employees in the recognition and handling of transactions suspected to be associated with money laundering.

Policy

The provisions of the Law have been adopted by the Company, which introduces procedures and processes that ensure compliance with the Law and Directives issued by Estonia Politseija Piirivalveamet and in line with the latest EU 5th AML Directive on this matter.

This AML Policy sets out the general measures which will apply to all clients such as:

- check the identity of the Client
- Verify the Client
- monitor any suspicious Client activities and/or transactions
- have a record of all the related information and/or documents of the Client's financial transactions

These procedures apply to the Back Office and detail the processes for the Company's KYC and due diligence procedures when accepting clients to open exchange accounts.

Restricted Business and Jurisdictions

Our Company does not provide services to clients that their activities are associated with any high risk or banned activities.

Furthermore, the Company does not accept clients from high risk countries, including but not limited to the following countries:

- Afghanistan
- Algeria
- American Samoa
- Bahamas

- Bangladesh
- Bolivia
- Bosnia and Herzegovina
- Botswana
- Brazil
- Cambodia
- China
- Colombia
- Congo
- Cuba
- Democratic People's Republic of Korea
- Ecuador
- Ethiopia
- Ghana
- Guam
- Iceland
- Indonesia
- Iran
- Iraq
- Japan
- Jordan
- Kyrgyzstan
- Laos
- Lebanon
- Libya
- Macau
- Malaysia
- Morocco
- Myanmar
- Nepal
- Nigeria

- North Macedonia
- Occupied Palestinian Territory
- Pakistan
- Panama
- Puerto Rico
- Samoa
- Serbia
- Somalia
- Sri Lanka
- Sudan
- Syria
- Taiwan
- Thailand
- Trinidad and Tobago
- Tunisia
- Uganda
- US
- US Virgin Islands
- Vanuatu
- Venezuela
- Vietnam
- Yemen
- Zimbabwe

Furthermore, the Company does not accept clients from high-risk countries as per the guidelines of FATF <http://www.fatf-gafi.org/countries/> which is updated accordingly.

B. KYC PROCEDURE

Client Identification and Due Diligence Procedures

The Company has adopted all requirements of the Law in relation to client identification and due diligence procedures. The client identification and due diligence are as follows:

➤ *Client Due Diligence Procedure*

Client Due Diligence procedure shall comprise the following:

- i. Identification of the client and verification of the client's identity on the basis of information obtained from a reliable and independent source. This is KYC procedure, which is explained in detail further below.
- ii. Identification of the beneficial owner and taking risk-based and adequate measures to verify his/her identity on the basis of documents, data or information issued by or received from a reliable and independent source. As regards to legal persons, trusts and similar legal entities, taking risk-based and adequate measures to understand the ownership and control structure of the client.
- iii. Obtaining information on the purpose and intended nature of the business relationship.
- iv. Conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the data and information held by the firm in connection with the client.

The KYC procedure is a requirement in order to comply with the International law provisions, including the ones designed to prevent money laundering. The following procedure should be followed unless an amendment is sent from the Compliance Department stating otherwise.

When a client applies to open an account with us it is the Company's duty to ensure that along with the application the following documents are received:

Natural Persons – (this also applies to natural persons involved in a legal entity such as Directors, Shareholders or authorized persons)

1. Proof of Identity (POI)

At least one of the following documentations need to be collected as proof of identification to perform a World-Check:

- Passport - A Clear Passport Full Copy (4 corners and MRZ lines)
- Identification Card ('ID')
- Driving License ('DL')

Notes:

1. For EU citizens an Identification card is adequate.
2. For 3rd country nationals where a passport is not available the Company must collect from client: 2 governmental identification such as ID and Driving license.

Once the POI had been provided, the following information shall be verified: Date of birth ('DoB') (the client needs to be over 18 years old)

Date of expiration of the document (if any, as some IDs don't have an expiry date).

The identity of each client whether he is a natural person, or a legal entity is checked against a respectable and worldwide accepted third party electronic database for business research and risk management services. Currently we are using 'Lexis Nexis'.

In addition, the Company must check if the document is genuine and report to the Compliance Officer if there are any doubts.

2. Proof of Residence (POR)

The following documents shall be accepted as proof of identification of a client residence. All documentation needs to be recent, up to 3 months:

- Recent Utility Bill. This can be water bill, electricity bill, bank statement or bank reference letter, tax bill, municipality bill where home address is shown or,
- Bank Statement or
- Local Authority Tax Bill or
- Any other official document same with the abovementioned.

In case on the POR it is written in a family member's name (parents or spouse) we must require a:

- Birth Certificate or Marriage Certificate to prove the relationship between the two individuals.

The below mentioned document cannot be considered as proof of residence (*unless exception is given by the Compliance Officer*):

- Mobile phone bill
- Insurance Statement
- Electronically generated documents.

Note that Proof of Identification and Address must be 2 different documents.

3. Proof of Signature

In the case that the Proof of Signature is needed, it can be obtained thru the passport or ID or DL. However, if the proof of signature is not on the Identification Document then the Company has the right to request from the Client to complete, sign and return a “Specimen Signature Form” (Appendix I).

4. Proof of Bank Account Ownership

If a new client wishes to exchange Cryptocurrency to FIAT, he must also provide proof of ownership of account. Such document is a bank statement where the name and the address match the company’s records

Corporate Accounts

When a legal entity wishes to open an account with Venus Exchange Services OÜ the below must be collected:

I. Company’s Incorporation Documents

- a. Certificate of incorporation or equivalent
- b. Certificate of registered office or equivalent
- c. Certificate of directors and secretary or equivalent
- d. Certificate of shareholders or equivalent
- e. Memorandum and articles of association of the legal person
- f. Recent copy (up to three months) of a bank statement or utility bill in order to verify the head office address
- g. Identity of Directors and Shareholders with their relevant KYC documents required of Natural Persons
- h. Authorized person resolution signed by the Board of directors (‘BoD’)

The company’s documentation must be recent (maximum 1 year)

Our Company does not accept legal clients where the shares are issued in a form of “Bear Shares”.

Additional Documents

Depending on the amount the client wishes to exchange, the Company has formed Tiers where the required documentation differ. These Tiers are:

Tier 1

- Up to 5,000
 - PoR
 - PoI

Tier 2

- 10,000 and more
 - PoR
 - PoI
 - Questionnaire

Recordkeeping

Assessment of client documents will be made on an annual basis. All client’s documents and record transactions will be kept safely and back-up for a minimum five (5) year period.

➤ Timing of identification

Client and beneficial owner identification must take place before the establishment of a business relationship or where applicable the carrying out of a transaction, receipt of funds to the accounts does not mean establishment of business relationship.

By way of derogation, the verification of the identity of the client and the beneficial owner may be completed during the establishment of a business relationship if this is necessary in order not to interrupt the normal conduct of business and where there is limited risk of money laundering or terrorist financing occurring. In such situation, these procedures shall be completed as soon as practicable after the initial contact.

➤ Renewal of client identification

Reviews of existing records must take place on a regular basis, thus ensuring that the documents, data or information held are kept up-to-date. Client due diligence procedures shall be applied not only to all new clients but also at appropriate times to existing repeated clients on a risk sensitive basis.

Enhanced Client Due Diligence

The Company should apply enhanced client due diligence measures in situations which by nature can present high risk of money laundering or terrorist financing.

More specifically, in cases as follows:

- where the client is from a country that has been identified as “Countries with Strategic Deficiencies” per the FATF, the Company shall take specific and adequate measures to compensate for the high risk, by applying one or more of the following measures:

- Ensuring that the client’s identity is established by additional documents, data or information.
- Supplementary measures to verify or certify the documents supplied or requiring confirmatory certification by a credit or financial institution.
- Ensuring that deposits are carried out through an account opened in the client’s name with a credit institution which operates in a country of the European Economic Area or a country where its AML policies are in line with the EU.
- For transfers to and from these countries, additional KYC of the sender or beneficiary and supporting documentation to document and justify the transfer will be required before execution.

- Politically exposed persons (“PEPs”) are individuals who are or have been entrusted with prominent public functions in a foreign country and close associate is someone with a close relationship with the political exposed persons. The Company should adopt the following additional due diligence measures to determine whether a prospective client is a politically exposed person:

- Approval from Senior Management prior to the establishment of a business relationship with the client.

- Take appropriate measures for the establishment of the origin of the client's assets and the source of funds that are related with the establishment of the business relationship or transaction.
- Conduct enhanced and continuous monitoring of the business relationship.

Enhanced Due Diligence procedure is elaborated further down.

C. Client Risk Assessment

Each Client who wishes to receive our services to exchange fiat to digital currency or the opposite shall be assigned to one out of following three categories:

Low Risk (Level I)

Individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile may be categorized as low risk. Examples of low risk customers may be salaried employees whose salary structures are well defined, individuals from the lower economic strata of the income level whose accounts show minimal balances and low turnover, regulators and statutory bodies etc. In such instances, only the basic needs of verifying the identity and location of the customer can be met.

Medium Risk (Level II)

Customers that are likely to pose a higher than average risk to the exchange may be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc.; such as:

- a) Persons in business/industry or trading activity where the area of his residence or place of business has a scope or history of unlawful trading/business activity.
- b) Where the client profile of the person/s opening the account, according to the perception of our Company is uncertain and/or doubtful/dubious.

High Risk (Level III)

The Company will apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear. The examples of customers requiring higher due diligence may include:

- High Net worth individuals
- Trusts, charities, NGOs and organizations receiving donations,
- Companies having close family shareholding or beneficial ownership
- Firms with 'sleeping partners'

- Politically Exposed Persons (PEPs) Those with dubious reputation as per public information available, etc.

The criteria used for risk assessment for this category are:

- Risk from the country of origin
 - Can be determine as per the geographical risk, i.e. risk from country of origin. The evaluation of the risk from country of origin is performed according to the following:
 - For natural persons: The residence country
 - For legal entities: The country in which is the legal entity's seat.

When referring to high risk countries, it refers to countries with high corruption index, unsecure economical and political systems, inefficient legal system or small number of requirements for the documentation needed for opening businesses, countries known for production, processing and trafficking drugs and weapons.

As additional factors that would influence the decision whether some country represents a risk, could be:

- States under sanctions, embargos or similar measures, issued, for example, from the United Nations
- States identified, by credibility sources, as states having incompatible regulation for prevention of money laundering and financing terrorism with the international regulation from this area,
- States identified, by credibility sources, as states financing and supporting terrorism
- Risk from a profile of a client
 - Can be determine when assessing a client based on the following criteria:
 - Significant and unexplainable geographic distance between the entity who should perform the activity and the place of residence or the seat of the client;
 - Frequent movements of funds in different accounts in various financial institutions;
 - Clients for which is difficult to identify the real owner (off-shore companies).
 - Activities that offer money services (remittances, exchange of foreign-exchangeable operations, services for fast money transfer, as well as other activities offering money transfer)
 - Casinos, betting shops and other activities related to the games of chance;
 - Charity organizations and other “non-profit” organizations which are not subject of a control (especially the ones acting across borders);
 - Bank accounts of accountants, lawyers or other professionals who act in the name of their clients, who by the financial institutions are treated as VIP clients;

Senior Management approval must be sought before establishing a relationship with such a person. It is also a requirement to establish the high risk client's source of wealth/source of funds and the beneficial owners.

Political Exposed Persons (PEP)

PEP is a person that meets one or more of the following criteria:

- a. heads of State, heads of government, ministers and deputy or assistant ministers;
- b. members of parliament or of similar legislative bodies;
- c. members of the governing bodies of political parties;
- d. members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances; members of courts of auditors or of the boards of central banks;
- e. ambassadors, chargés d'affaires and high-ranking officers in the armed forces;
- f. members of the administrative, management or supervisory bodies of State owned enterprises; directors, deputy directors and members of the board or equivalent function of an international organization.

Where a PEP is no longer entrusted with a prominent public function, financial institutions must consider the continuing risk posed by affiliation with such PEP for at least 12 months (or longer, until the Company determines that the risk specific to such PEP has diminished).

D. Source of Funds

For High Risk clients, whether these are legal entities or individuals, the Company further to the enhance due diligence as per the previous section, will apply the request for the following documentation (whatever applicable) in order to identify the source of funds.

In addition, Source of funds is requested for all clients that wish to make transactions equivalent to €10,000 and above. This amount can be accumulated or one time deposit.

For Individuals

- Curriculum Vitae ("CV") – This applies to individuals as it will make it possible to trace the career of the client and to better target the search for information as to the origin of the funds. This will allow us to establish a picture of where the client's earnings derived from.
- Bank Statements of last six months

- Previous year/s Tax reports
- Tax payment
- Income certificate
- Full payslip or other documents confirming salary
- Inheritance (stamped grant of probate, stamped grant of letters of administration)
- Sales and purchase agreements
- import and export related documents for the shipment of goods
- Reliable media
- Publicly available databases

Furthermore, the Company can obtain when applicable publicly available information on the internet. Same applies to the Legal entities section below.

For Legal Entities

- Audited Financial Statements – for newly formed companies, latest management accounts
- Bank Statements of last six months
- Loan Agreements if applicable
- Sales and purchase agreements

Transfer of funds

General Practice

When transferring money for purchasing digital currency, the sender's name and the information held on file provided by the Client upon the agreement, should match.

Money transfers from another party other than the account holder is strictly prohibited. Furthermore, we will refuse any third-party transfers towards one of our Clients.

In case there is any discrepancy on a transaction, we reserve the right to automatically cancel or suspend the transaction. Further to this, third parties are forbidden to conduct the transaction in replace of the Client.

Likewise, the information about transferring digital currency for sale, the recipient's name and the account holder has to be the same. Transferring through the online payment system is allowed ONLY at the same account and/or wallet from where it was first used.

1. Credit Card transactions

To ensure that the owner of the account matches the cardholder, we ask that the client sends to us a clear coloured copy of the card. For security reasons, we ask that the 8 middle digits of the card number used for the transaction for all amounts are covered. We ask that the credit card is a valid credit card where the name of the card holder is shown.

Not card will be accepted where it does not bear a name of the owner. Such example is a prepaid card or internet card. In such cases the money will be rejected and send back to the sender.

2. Wire Transfers

When client is making a wire transfer, he is requested to provide the company with proof of the wire transfer for 2 reasons:

- a. To eliminate any possibility of errors such as wrong client
- b. To be alerted for incoming funds

Important Notes

- Have the Senior Management approval prior of opening a “Political Exposed Person” account.
- When a PEP is a potential client, we need to obtain a bank reference letter.
- Where the documents are not in English:
 - We need translation from a translator (external and/or an employee of the Company).
 - If there is no one to translate the documents, we ask the client to send us an official translation from a notary.

Venus Exchange Services OÜ has the right to refuse any client without giving reason.

Appendix I

I, (insert your name as it is on
the exchange account) hereby enclose a specimen signature to www.btc-land.com an
exchange digital currency platform owned by Venus Exchange Services OÜ .

Date: -----