

## INTRODUCTION

This is an Anti-money laundering (hereinafter referred to as: “AML”) and Counter-terrorist financing (hereinafter referred to as: “CTF”) Policy, which Alcor Exchange applies to its service.

The procedures are monitored by the compliance officer and his team. The compliance team monitors the compliance of the internal rules and procedures with the relevant laws and compliance of the activity of the Representatives with the procedures established by the Rules.

As per definition from our AML policy we do not work with offshore banks and shell banks, casinos and gaming industry or with any country listed as “High risk”.

## AML/CTF FRAMEWORK

Alcor Exchange has implemented measures, which protect Alcor Exchange from involvement in money laundering or terrorist financing activities (hereinafter: “suspicious transactions”), by:

- performing compliant due diligence procedure (the KYC) for every user who registers on the platform,
- making risk assessment for every user that successfully passed the KYC,
- detecting suspicious transactions by risk categories and risk levels,
- monitoring suspicious transactions,
- reporting suspicious transactions to the authorities.

In order to protect us and our users from the possible financial crimes, Alcor Exchange shall:

- Perform Know Your Customer procedures on all users and clients (natural and legal persons) on a regular basis.
- Perform an enterprise-wide risk assessment to determine the risk profile of the Company.
- Implement internal controls throughout its operations that are designed to mitigate risks of money laundering and terrorism financing.
- Conduct an periodic AML audit.
- Provide AML training to its employees.

## THE KYC AND RISK ASSESSMENT

In the user due diligence process, Alcor Exchange shall perform a KYC for every:

- User – a natural or legal person;
- Representative of the User – an individual who is authorized to act on behalf of the User;

- Beneficial Owner of the User;
- Politically exposed person (“PEP”) or a person connected with the PEP.
- During the registration procedure, every user must provide to Alcor Exchange with several personal information and documents, which Alcor Exchange need to establish a portfolio of the user and access the risk, connected to it.

KYC procedure could include PEP checks be performed with the usage of third party services such as but not limited to:

- Sum & Substance <https://sumsub.com/>
- Amlexa <https://www.amlexa.com/>
- Trulioo <https://www.trulioo.com/>

A politically exposed person of national level can be identified using the NameScan database: <https://namescan.io/FreePEPCheck.aspx> , which has a free access, or in any paid database (for example, Thomson Reuters, MemberCheck and others).

While checking a politically exposed person of local level, as well as a politically exposed person of national level, it is necessary to perform an additional check up using Google, and also using local search systems in the country of origin of the customer, by entering the customer's name and date of birth both in Latin letters and using the local language.

The decision to establish a business relationship with a politically exposed person of national level must be taken by the management board of the obliged entity, the responsible member of the management board or the contact person. If a business relationship is established with the customer that will become later on or later it will becomes known that he or she or actual beneficial owner has become a politically important person of state level in the understanding of this guidance, then it is necessary to inform the management board, the responsible member of the management board or the contact person.

**NATURAL PERSON NEEDS TO PROVIDE AT LEAST:** First name, last name; Date of birth, place of birth; Home address; Phone number and email; Government issued ID document (both sides); Other information and documents on the request of Alcor Exchange.

**LEGAL PERSON NEEDS TO PROVIDE AT LEAST:** Business name of the legal person; Registry code or registration number and the date of registration; ID of the shareholders (same as for the natural person identification), ID of the director(s) and/or members of the management board (same as for the natural person identification), ID's of the representatives (same as for the natural person identification); Proof of the registered office/seat; ID's of the beneficial owners (same as for the natural person identification); Bank statement; Proof of representation; Articles of association; Other information and documents on the request of Alcor Exchange.

Alcor Exchange makes sure to protect users personal data in accordance with the relevant laws and the Privacy policy.

## RISK LEVELS

The risk is divided to 3 LEVELS:

### **NORMAL**

The risk level is normal, there are no high risk characteristics present.

## **HIGH 1**

1. User is from high risk country.
2. User is local PEP or a person. associated with a PEP.
3. The legal person's area of activity is associated with enhanced money-laundering risk.
4. The legal person is situated in a country, which is listed in the list of risk countries.
5. The legal persons activities and liability are insufficiently regulated by law, and the legality of financing of which is not easy to screen.
6. The representative or the Beneficial Owner / Shareholder of a legal person is a local PEP or his / her family member.

## **HIGH 2**

1. User is suspected to be or to have been linked with a financial offence or other suspicious activities.
2. User is a non-resident individual, whose place of residence or activities is in a country, which is listed in the list of risk countries.
3. The representative or the Beneficial Owner / Shareholders of a legal person is a PEP or his or her family member
4. There is information that legal person is suspected to be or to have been linked with a financial offence or other suspicious activities
5. A legal person registered outside the European Economic Area, whose field of business is associated with a high risk of Money Laundering, or registered in a low tax rate country.

# RISK CATEGORIES

## **RISK BY USERS:**

Suspicious facts such as but not limited to the: discrepancies in provided id documents, fictitious person, stolen identity, counterfeited id document, post box home address, previous financial crime record, terrorist record, wanted person, no contact phone number, not valid documents, discrepancies in provided documents for the legal person, etc.

Politically exposed persons such as but not limited to the: prominent public functions: head of state, head of government, minister and deputy or assistant minister; a member of parliament or of a similar legislative body, a member of a governing body of a political party, a member of a supreme court, a member of a court of auditors or of the board of a central bank; an ambassador, a chargé d'affaires and a high-ranking officer in the armed forces; a member of an administrative, management or supervisory body of a state-owned enterprise; a director, deputy director and member of the board or equivalent function of an international organisation, except middle-ranking or more junior officials.

## **RISK BY COUNTRIES:**

Country of residence / nationality is a country with prohibition/restriction on cryptocurrencies such as but not limited to: Afghanistan, Algeria, American Samoa, Bangladesh, Bolivia, China, Democratic Republic Of Congo, Democratic People's Republic Of Korea (Dprk), Ecuador, Egypt, Ethiopia, Fyr Macedonia, India, Iran, Iraq, Kyrgyzstan, Pakistan, Palestine, Qatar, Saudi Arabia, Syria, Morocco, Nepal, United States Of America, Vanuatu, Vietnam, Zambia.

Resident / Citizen Of The High Risk Countries such as but not limited to: Bahrain, Yemen, Jordan, Kuwait, Lebanon, Libya, Malaysia, Mali, Mauritania, Nigeria, Oman, Somalia, Serbia, Sri Lanka, Sudan, Tunisia,

Turkey, Ethnic Groups Of Caucasus Belonging To Russian Federation (Chechens, Etc.), Trinidad & Tobago.

Low Tax Or Tax-free Countries such as but not limited to: United Arab Emirates, Oman, Bahrain, Qatar, Saudi Arabia, Kuwait, Bermuda, Cayman Islands, The Bahamas, Brunei, Vanuatu, Anguilla, Belize, Costa Rica, Guatemala, Panamá, Nicaragua.

### **RISK BY TRANSACTIONS**

Alcor Exchange shall inspect any outstanding transaction, which include but is not limited to the: large transactions that do not correspond to user's source of funds and/or source of wealth, transactions to offshore or shell bank (financial institution that does not have a physical presence in any country), executing payment via non-licensed payment institution, large daily movements of fiat or virtual money, etc.

### **RED FLAGS**

- Customer shows an unusual interest in AML policy and the relationship of policy to his personality, type of business or his source of funds.
- Customer involved in transactions that have no business purpose.
- Upon request, the client refuses or finds it difficult to indicate the source of the income or wealth.

## **FUNDING LIMITS**

Individuals and companies who have verified their accounts will be allowed to carry out deposit and/or withdrawals under the following limits, above which they will have to get in touch with Alcor Exchange's support staff:

|                        | <b>Daily Limits</b> | <b>Monthly Limits</b> |
|------------------------|---------------------|-----------------------|
| <b>Deposit Fiat</b>    | 20.000,00 EUR       | 50.000,00 EUR         |
| <b>Deposit Crypto</b>  | No Limit            | No Limit              |
| <b>Withdraw Fiat</b>   | 20.000,00 EUR       | 50.000,00 EUR         |
| <b>Withdraw Crypto</b> | 20.000,00 EUR       | 50.000,00 EUR         |

In any case, if Alcor Exchange identifies any suspicious transactions, it will ask the customer for more information or documentation, and if necessary, a report will be filed with the Reporting Office.

For both personal and corporate accounts, the deposits and withdrawals of Fiat will only be allowed from and to their own bank accounts, and never to third party accounts.

## **DETECTION OF SUSPICIOUS TRANSACTIONS**

Alcor Exchange shall diligently monitor transactions for suspicious activity. Transactions that are unusual will be carefully reviewed to determine if it appears that they make no apparent sense or appear to be for an unlawful purpose.

Implemented internal controls will serve as ongoing monitoring system in order to detect the suspicious activity or transaction. When such suspicious activity is detected, Alcor Exchange shall determine whether

a filing with any law enforcement authority is necessary. Suspicious activity can include more than just suspected money laundering attempts. Activity may be suspicious, and Alcor Exchange may wish to make a filing with a law enforcement authority, even if no money is lost as a result of the transaction.

Alcor Exchange shall initially make the decision of whether a transaction is potentially suspicious. Once Alcor Exchange has finished the review of the transaction details, he or she will consult with its management to make the decision as to whether the transaction meets the definition of suspicious transaction or activity and whether any filings with law enforcement authorities should be filed. Alcor Exchange shall maintain a copy of the filing as well as all backup documentation. The fact that a filing has been made is confidential. No one, other than those involved in the investigation and reporting should be told of its existence. In no event should the parties involved in the suspicious activity be told of the filing.

## REPORTING REQUIREMENTS

Reasonable procedures for maintaining records of the information used to verify a person's name; address and other identifying information are required under this Policy. The following are required steps in the record keeping process:

- Alcor Exchange shall maintain a record of identifying information provided by the user.
- Where Alcor Exchange relies upon a document to verify identity, Alcor Exchange shall maintain a copy of the document that the Company relied on that clearly evidences the type of document and any identifying information it may contain.
- Alcor Exchange shall also record the methods and result of any additional measures undertaken to verify the identity of the user.
- Alcor Exchange shall record the resolution of any discrepancy in the identifying information obtained.
- All transaction and identification records will be maintained for a minimum period of five years.

## TRAINING OF EMPLOYEES

- Responsibility for training of the employees of the private limited company on the prevention of money laundering and terrorist financing and compliance with international sanctions rests with the Contact person or employee appointed by the management board or a specialist in the field.
- Training is carried out as needed, but not less than once a year.
- The employee confirms participation in the training with his/her signature.
- The contact person has the right to make proposals to the management board of the institution regarding the educators.