

Know Your Customer Policy

1. General Terms

- 1.1. Know Your Customer Policy (KYC Policy) is an integral and inseparable part of the FortFC ICO Terms and Conditions.
- 1.2. The KYC Policy of FortFC (Company) lays down the basic guidelines for identification of clients (for natural persons) or their representatives (for legal entity).
- 1.3. The purpose of the KYC Policy is to establish requirements for the implementation of measures intended to be used for identification and analysis of clients' (for natural persons) or their representatives' (for legal entity) activities prior to establishing, and while maintaining, a relationship with them in order to avoid establishing a relationship with persons engaged in activities connected with money laundering and terrorism financing, which can result in reputational, financial or legal risks for the Company.
- 1.4. The KYC policy has been developed in accordance with international standards on combating crime, money laundering and terrorism financing.
- 1.5. The KYC Policy is applied both prior to establishing (during registration on the Company website) and while servicing the Client.
- 1.6. The KYC Policy sets minimum standards the Company must comply in accordance with the international requirements.

2. Studying Client's Activities

- 2.1. Application of Know Your Customer Policy

2.1.1. One of the key elements of the KYC Policy is a client identification procedure.

2.1.2. The Company carries out the identification procedure in the following circumstances:

- prior to establishing a relationship with the Client (during registration on the Company website);
- during the verification of the Client's personal data;
- during the verification of the Client's payment details;
- while processing the Client's funds withdrawing request;
- if there is a suspicion that the Client is involved in activities connected with money laundering and terrorism financing;
- if there are doubts about the veracity or relevance of the previously obtained Client identification data;
- as part of scheduled and unscheduled updates of the Client's payment details and personal data.

2.1.3. The scope and scale of measures carried out as part of the KYC Policy depend on the nature of the Client's activity and the level of potential risk he/she poses to the Company. If the Client's activity poses elevated risk, the Company may undertake enhanced Client identification procedures.

2.1.4. The Client identification procedure consists of the following steps:

- identification of the Client (for natural persons) or his/her representative (for legal entity);
- specifying the legal entity ownership and management structures, including its ultimate owners;
- searching for information about the Client or his/her representatives in public information sources;

- assessing the risk level of the Client's financial transactions.

2.2. Client Identification

2.2.1. The clients are required to provide up-to-date identification information and notify the Company of any changes in their contact or personal information within ten (10) calendar days of occurrence thereof.

2.2.2. Identification of natural persons involves obtaining the following information:

2.2.2.1. During registration of the Client on the Company website:

- first and last name (in some cases, the middle name);
- place of temporary residence;
- place of residence (registration);
- phone number registered and used by the Client;
- e-mail address registered by the Client and used for receiving information from the Company.

2.2.2.2. During the verification process in the Personal cabinet the Client provides the following documents:

- primary document - a passport or national ID card (except the corporate access cards) issued by the government of the client's jurisdiction, driver's license (for countries where driving license is a primary identification document). The validity of the document must exceed the period of FortFC ICO campaign.
- Additional document (a document confirming the Client's registration address, i.e. a page in the passport with a residence stamp, driving license, bank statement, utility or other bills containing the Client's name and issued not earlier than four (4) months prior to the Client account registration date).

2.2.3. Identification of legal entities involves obtaining the following information:

2.2.3.1. During registration of the Client on the Company website:

- legal entity's official name;
- legal entity's registration address;
- authorized representative's phone number;
- company's e-mail address or e-mail address registered on the authorized person's name for receiving information from the Company.

2.2.3.2. During the verification process in the Personal cabinet the Client provides the following documents:

- Company Registration Document (certificate of registration of a legal entity);
- Certificate of the company good standing (issued not earlier than 6 months);
- Certificate of Ownership of the Company;
- Certificate of Incumbency, specifying the names of the directors and shareholders;
- a document confirming the appointment and powers of the director (if the company has two (2) or more directors, a confirmation of the right of one of the directors to sign documents on behalf of the company);
- copies of all company directors' passports and their addresses;
- Power of Attorney issued by the company director to an employee or by company owners to the director, authorizing the official representative to act on behalf of the legal entity in order to conduct transactions on international financial markets through FortFC;

- Authorized person's passport, or any other identification document issued by the government of the authorized person's jurisdiction. The validity of the document must exceed the period of FortFC ICO campaign;
- a document confirming the authorized person's registration address, i.e. a page in the passport with a residence stamp, driving license, bank statement, utility or other bills bearing the Client's name and issued not earlier than four (4) months prior to the Client account registration date).

2.2.3.3. If there are suspicions that the legal entity is involved in activities connected with money laundering and terrorism financing, FortFC may suspend this Client's financial activity on the company accounts and request additional identification documents, e.g. company incorporation documents (memorandum and articles of association); information on the company's contractors; brief information about the state of the business; information on participation in associations of legal persons; information on the legal person's involvement in arbitration proceedings; and other documents requested by the Company manager.

2.2.4. The Company's clients (legal entities) must pass the verification of payment details in Personal cabinet, specifying the payment details they intend to use for credit and debit transactions.

3.Transaction Restrictions

3.1. The Company does not open accounts for anonymous owners (i.e. without providing primary information during registration on the Company website).

3.2. The Company reserves the right to block the client's Personal cabinet\suspend Client's activity\refuse withdrawal of the Client's funds in case of:

- failure to submit identification documents at the expiration of ten (10) calendar days from the date of registration of the Client on the Company's website;
- failure to provide information about changes in the contact or personal information at the expiration of ten (10) calendar days after occurrence thereof;
- absence from its principal place of business of a legal entity, its permanent governing body, other body or person authorized to act on behalf of such legal entity without power of attorney;
- provision of false identification documents by the Client;
- if there is information pointing at the involvement of the Client (owners or directors for legal entity) in criminal activities, extremism, financing terrorism or money laundering.

4. Data Storage

4.1. The Company retains the information received during the Client's identification and security analysis for at least 5 years from the date of termination of the relationship with the Client, regularly updating it and keeping in a place allowing its easy retrieval.

4.2. The Company retains the following information concerning each Client:

- contact information (phone number, e-mail address);
- documents and information received in the process of Client identification;

- information about the Client's key characteristics, such as characteristics of activities, the source of funds, the reasons and purpose of account opening (for legal entities);
- documents and information received during scheduled and unscheduled inspections of the Client and analysis of his activity.

5. Client Monitoring

5.1. The Company conducts an ongoing monitoring of the Client's transactions in order to ensure timely detection of transactions subject to mandatory monitoring and suspicious transactions.

5.2. Suspicious transactions include:

- currency exchange transactions not linked to any trading activity;
- account transactions or other activity that is different from the one stated in the company's incorporation documents;
- transactions which have no apparent economic sense.

5.3. Company employees involved in maintaining a relationship with clients conduct an ongoing daily monitoring of their transactions to identify unusual and suspicious transactions/activity. Upon detection of such transactions/activity, a Company employee will forward this information to the Compliance Manager, who will conduct additional analysis and, if necessary, report the transaction details to the Competent Authority.

5.4. The Compliance Manager is responsible for advising and training the Company employees involved in maintaining relationship with clients to be able to identify transactions possibly linked to money laundering and terrorism financing and



recognize indicators suggesting that the sources of the Client's funds need to be studied in greater details.