Version dated May 15, 2019

# AML and KYC Policy

BIT TRADE MARKETS OÜ, a company duly incorporated in Estonia (Company ID code 14555301) (hereinafter the "Company"), represents its Anti-Money Laundering and Know Your Customer Policy (hereinafter the "Policy"), which is designated to prevent and mitigate possible risks of the Company being involved in any kind of illegal activity.

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 Customers.

This Policy represents the provisions of AML and KYC Policy and regulates verification procedures, activities of compliance officers, transaction monitoring and risk assessment.

CONTENTS



## 1. TERMS AND DEFINITIONS

**1.1.** **Personal Data** means any information directly or indirectly related to a specific or designated Customer and/or Internet User.

**1.2.** **Processing of Personal Data** means any action (operation) or set of actions (operations) performed using automation tools or without using such tools with Personal Data, including collection, recording, systematization, accumulation, storage, clarification (updating, modification), extraction, use, transfer (distribution, provision, access), depersonalization, blocking, deletion, destruction of Personal Data and other actions.

**1.3.** **Confidentiality of Personal Data** means a mandatory requirement for the Company to prevent the dissemination of Personal Data without the consent of the Customer and/or Internet User or without any other legal basis.

**1.4.** **Customer** means a natural or legal person that uses the Services, which comply with these terms and conditions, is the holder of the Account, has successfully completed all KYC procedures, and is confirmed by an officer of the Company.

**1.5.** **Internet User** means a natural person who uses the Site.

**1.6.** **Products/Services** mean all and any Products and Services provided by the Company.

**1.7.** **Customer Account** means a set of Customer's details required for his/her authentication, authorization and gaining access to the list of the Company's Products and Services determined by the appropriate Account level.

**1.8.** **Account** means an account registered by the User on the Site.

**1.9.** **Site** means the website of the platform at https://bit.trade functioning in the interests of BIT TRADE MARKETS OÜ.

## 2. VERIFICATION PROCEDURES

**2.1.** 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 AML and KYC Policy.

## 3. IDENTITY VERIFICATION

**3.1.** The Company's identity verification procedure requires the Customer to provide the Company with reliable, independent source documents, data or information (e.g., national ID, international passport, bank statement, utility bill). For the AML and KYC Policy purposes, the Company reserves the right to collect the Customer's Personal Data.

**3.2.** The Company shall take steps to confirm the authenticity of documents and information provided by the Customers. All legal methods for double-checking Personal Data shall be used, and the Company reserves the right to investigate certain Customers who have been determined to be risky or suspicious.

**3.3.** The Company reserves the right to verify the Customer's identity in an on-going basis, especially when the Customer's Personal Data has been changed or his/her activity seemed to be suspicious (unusual for the particular Customer). In addition, the Company reserves the right

to request up-to-date documents from the Customers, even though they have passed identity verification in the past. The Personal Data is processed strictly in accordance with the Privacy Policy and the regulations of the Company.

**3.4.** Once the Customer'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.

**3.5.** The Company does not provide Services to citizens and/or residents of the United States of America (USA).

## 4. CARD VERIFICATION

**4.1.** The Customers and Internet Users, who intend to use payment cards in connection with the Company's Products and Services, have to pass card verification in accordance with the instructions available on the Company's Site.

## 5. COMPLIANCE OFFICER

**5.1.** The Compliance Officer is the person, duly authorized by the Company, whose duty is to ensure the effective implementation and enforcement of this Policy. It is the Compliance Officer's responsibility to supervise all aspects of the Company's Anti-Money Laundering and counter-terrorist financing, including but not limited to:

- Collecting Personal Data of Customers and Internet Users;
- 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;
- Monitoring transactions and investigating any significant deviations from normal activity;
- Implementing a records management system for appropriate storage and retrieval of documents, files, forms and logs;
- Updating risk assessment regularly;
- Providing law enforcement with information as required under the applicable laws and regulations.

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

## 6. TRANSACTION MONITORING

**6.1.** The Customers are known not only by verifying their identity (who they are) but, more importantly, by analyzing their transactional patterns (what they do). Therefore, the Company relies on data analysis as a risk-assessment and suspicion detection tool. The Company performs a variety of compliance-related tasks, including capturing data, filtering, record-keeping, investigation management, and reporting. The System functionalities include:

- daily check of Customers against recognized "black lists" (e.g. OFAC), aggregating transfers by multiple data points, placing Customers on watch and Service denial lists, opening cases for investigation where needed, sending internal communications and filling out statutory reports, if applicable;
- document management;
- tracking Customer behavior patterns.

**6.2.** With regard to this Policy, the Company shall monitor all transactions, and it reserves the right to:

- ensure that transactions of suspicious nature are reported to the proper law enforcement through the Compliance Officer;
- request the Customer to provide any additional information and documents in case of suspicious transactions;
- suspend or terminate Account when the Company has reasonable suspicion that the Customer is engaged in illegal activity;

**6.3.** The above list is not exhaustive, and the Compliance Officer shall monitor Customers' transactions on a day-to-day basis in order to define whether such transactions are to be reported and treated as suspicious or are to be treated as bona fide.

## 7. RISK ASSESSMENT

**7.1.** The Company, in line with the international requirements, has adopted a risk-based approach to combating money laundering and terrorist financing. By adopting a risk-based approach, the Company is able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate to the identified risks. This will allow resources to be allocated in the most efficient ways. The principle is that resources should be directed in accordance with priorities so that the greatest risks receive the highest attention.

## 8. COMPULSORY CONDITIONS

**8.1.** The Company, at its sole discretion, shall make changes and amendments to this Policy.

**8.2.** Notwithstanding the validity of this Policy in writing, its electronic version placed on the Site shall prevail.

**8.3.** This Policy is translated into English and/or other languages for convenience only. In case the interpretation of the original version of this Policy (its translation into English and/or other languages) differs from English, the Russian version shall prevail.

**8.4.** Whenever the context shall require, all words herein in the masculine gender shall be deemed to include the feminine or neutral genders, all singular words shall include the plural, and plural words shall include the singular.

**8.5.** The right to interpret the provisions of this Policy as well as the right to change the interpretations belongs exclusively to the Company.

**8.6.** Any other interpretation of the Policy given by the Customer and/or Internet User or non-compliance with these terms, conditions and procedures shall be unacceptable.