ANTI-MONEY LAUNDERING AND KNOW YOUR CUSTOMER POLICY (HEREINAFTER — "AML AND KYC POLICY")

Bit Trade Markets Limited (registration number 2499449) registered at 19H Maxgrand Plaza, No.3 Tai Yau Street, San Po Kong, Kowloon, Hong Kong (hereinafter referred to as the "Company") presents this Anti-Money Laundering and Know Your Customer Policy (hereinafter referred to as the "Policy") intended for preventing and mitigating possible risks for the Company related to its involvement in illegal activities of any kind.

According to both international and national standards, the Company is required to implement efficient internal procedures and mechanisms for preventing money laundering, terrorist financing, drug and human trafficking, proliferation of weapons of mass destruction, corruption and bribery, as well as to take actions in the event of any suspicious actions of the Website User.

Money laundering is actions aimed to conceal or hide the true source of criminally acquired income and its further legitimization.

The Company actively counteracts any form of money laundering activity. This Policy is designated for the Company to follow the standards for preventing the Website Users to use its products and services for money laundering.

This Policy governs activities of the Compliance officers, as well as verification procedures and risk assessment.

Contents:

1. VERIFICATION PROCEDURES

1.1. One of the international standards for preventing illegal activities is the Website User due diligence (CDD — Customer Due Diligence). According to CDD, the Company establishes its own verification procedures within this Policy.

1.2. Identity Verification

1.2.1. Taking anti-money laundering measures, the Company requires the Website Users to provide appropriate documents that confirm their identity and source of income to acquire corresponding products and services.

1.2.2. The Company's identity verification procedure requires the Website User to provide the official, independent source documents or information (e.g., national ID, international passport, bank statement or utility bill). For the purposes of this Policy, the Company reserves the right to inquire the Website User's personal data. The Company shall take steps to confirm the authenticity of documents and information provided by the Website Users. The Company shall take all legal measures to verify identification data. The Company reserves the right to collect information about the Website Users who have been determined to be risky or suspicious.

1.2.3. The Company is not authorized and obliged to ascertain whether the document the Website User provides for identification is legal. However, in the event of evident inconsistency of the received information, the Company has the right to demand additional identification documents from the Website User. If the Website User refuses to provide the required information, when needed, or tries to mislead the Company, such a Website User may be denied in providing the services.

1.2.4. The Company reserves the right to verify the Website User's identity on an on-going basis, especially when the Website User's personal data has been changed or his/her activities seemed to be suspicious (unusual for the particular Website User). In addition, the Company reserves the right to request up-to-date documents from the Website Users, even though they have passed identity verification in the past.

1.2.5. The Website User's personal data is collected, disclosed and protected strictly in accordance with the Bit Trade Website Privacy Policy.

1.2.6. Once the Website User's identity has been verified, the Company may relieve itself of potential legal liability in a situation where its services and/or products are used by the Website User to conduct illegal activities.

1.2.7. If the Company reveals suspicious activities of the Website User related to money laundering, terrorist financing, illegal drug and human trafficking,

proliferation of weapons of mass destruction, corruption and bribery, the information about such activity shall be reported to the relevant authorities.

2. COMPLIANCE OFFICER

2.1. The Compliance Officer is a person duly authorized by the Company, whose duty is to ensure the efficient implementation of and compliance with this Policy. It is the Compliance Officer's responsibility to supervise all aspects of the Company's anti-money laundering and counter-terrorist financing policy, including but not limited to:

- collecting personal data of the Website Users;
- establishing and updating internal policies and procedures for the completion, review, submission and storage of all reports and records required under the applicable laws and regulations;
- monitoring transactions of the Website User and investigating any significant deviations from normal activity;
- implementing a record management system for appropriate storage and retrieval of documents, files, forms and logs;
- updating risk assessment regularly;
- providing law enforcement authorities with the necessary information as required under the applicable laws and regulations.

2.2. The Compliance Officer is entitled to interact with the law enforcement authorities involved in prevention of money laundering, terrorist financing and other illegal activities.

3. TRANSACTION MONITORING

3.1. The Website Users are verified by establishing their identity, as well as by analyzing their transaction patterns. Therefore, the Company relies on data analysis as a risk-assessment and suspicious activity detection tool. The Company performs a variety of compliance-related tasks, including collecting and organizing data, record-keeping, investigation management and reporting. The functionality of the compliance includes:

- Daily checks of the Website Users for recognized "black lists" (e.g. OFAC), aggregating transfers by multiple data points, placing the Website Users 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 Website Users' behavior patterns.

In accordance with this Policy, the Company shall monitor all actions and reserves the right to:

- report on suspicious actions to law enforcement authorities;
- request the Website User to provide any additional information or documents in the event of suspicious actions;
- suspend or terminate the Website User's Account when the Company has reasonable suspicion that the Website User is engaged in illegal activities;

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

4. RISK ASSESSMENT

In accordance with the international requirements, the Company has applied a risk-based approach to combating money laundering and terrorist financing. In this way, the Company is able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate to the identified risks, which is one of its priorities. This will allow the resources of compliance system to be allocated in the most efficient way. The principle is that resources should be directed in accordance with priorities so that the greatest risks receive the highest attention.

5. GENERAL PROVISIONS

In the case of the arising questions regarding this Policy, one should contact the Support Service on the Website.

Changes and additions to this Policy may be made solely by the Company.

In case of any discrepancies between different versions of this Policy (printed, electronic, etc.), the electronic version of this Policy currently available on the Website shall be deemed the official one.

The translation of this Policy into other languages is available on the Website for Website Users' convenience only. In case of any differences in interpretation hereof, the version in Russian shall prevail.