

Anti-Money Laundering and Know Your Customer Policy

The BITmarkets Anti-Money Laundering and Know Your Customer Policy (“AML/KYC Policy”) outlines a comprehensive framework to provide protection against financial crimes, fraud, and other illicit activities, and is intended to prevent and minimize the potential risks and the likelihood of BITmarkets from being linked to unlawful activities and to ensure compliance with the rules and regulations. BITmarkets is fully aware of the serious impact and the detrimental effects of financial crimes and is dedicated to operating and maintaining ethical business practices. BITmarkets prioritizes the protection of its clients, workforce, and all individuals and entities that BITmarkets is associated with. Further, to contribute to the efforts of preventing and addressing financial crime, BITmarkets actively supports the government, law enforcement agencies and the regulatory bodies.

The law mandates that all obligated entities must collect, verify, and document information to identify individuals or entities seeking to establish business relationships or conduct occasional transactions with BITmarkets. This AML/KYC Policy establishes stringent measures, including but not limited to, risk assessment, customer due diligence, on-going customer diligence, reporting obligations of BITmarkets to the authorities, sanctions, and record keeping.

- I. BITmarkets adopts a risk-based approach, which involves the identification, documentation, and assessment of risks that need to be addressed. BITmarkets conducts an assessment and evaluation of the risks it faces in relation to the services it is authorized to offer. The specific circumstances determine the appropriate procedures and measures to be implemented in order to address and mitigate potential risks taking into account the following categories:
 1. Client’s nature;
 2. Client’s behavior;
 3. Client’s services and financial instruments;
 4. The risks with regard to communications, channels, products and services, geographic area and jurisdictions.
- II. The Client Due Diligence (“CDD”) measures are required to verify the identity of a new or existing client of the Company in order to recognize and mitigate risks such as, but not limited to, money laundering, terrorist financing, and other illegal activities. These measures also include levels of due diligence measures whereby the identification and application of Enhanced Due Diligence (“EDD”) for higher-risk clients and the detection of Politically Exposed Persons (“PEPs”) is applied to ensure appropriate risk management and compliance with regulatory requirements. The following CDD outlines the criteria that must be adhered to at all times:

1. Identification and verification of the prospective or existing client using reliable and independent source documents, data, or information;
2. Verification and identification of the individual claiming to act on behalf of the prospective or existing client, ensuring they are duly authorized to do so;
3. Identification of the beneficial owner and the implementation of reasonable measures to verify their identity using relevant information or data obtained from a reliable and independent source, ensuring that the reporting institution is satisfied in accurately identifying the beneficial owner;
4. Understand and, where applicable, obtain information about the purpose and intended nature of the business relationship;
5. If a prospective client fails to provide complete information and documents, the trading account will not be verified.

For individual applicant, BITmarkets is required by law to request information regarding the following:

1. Personal contact and identification details;
2. Employment information;
3. Source of funds;
4. Bank information; and
5. Copies of documents that validate the information mentioned above.

For corporate applicant, BITmarkets is required by law to request information regarding the following:

1. Corporate documents;
2. Management information;
3. Identification of the ultimate beneficial owner;
4. Identification documents;
5. Source of funds and/or source of wealth;
6. Authorization letter granting individuals the authority to act on behalf of the corporate entity;
7. Copies of documents that validate the information mentioned above; and
8. Filling out the KYC Questionnaire form.

BITmarkets refrains from initiating or continuing business relationships or conducting transactions in the following situations when:

1. BITmarkets is unable to fulfill the necessary Client CDD requirements;
2. The client or ultimate beneficial owner fails to provide complete, accurate, or updated information and documentation;
3. Indications or suspicions of BITmarkets' services could be exploited for illegal activities;
4. The client or transaction involves jurisdictions, industries, or entities subject to international sanctions or high-risk designations;
5. The risk profile or the transaction's risk level exceeds BITmarkets established risk threshold;
6. The client or transaction exhibits red flags associated with illegal activities; or

7. The client refuses to disclose the purpose of the business relationship or transaction.
-
- III. The On-Going Customer Due Diligence (“ODD”) is required for the continuous review, as well as to scrutinize and ensure that the account and transactions are consistent with the information, profile, and source of funds provided, and are in line with the intended purpose of the business relationship.
 - IV. BITmarkets is required by law to report suspicious transactions and activities to the relevant authorities. All data and information obtained for this purpose shall be safeguarded in such a way that only authorized employees have access to the information and documentation as well as in accordance with the applicable AML/CTF laws or regulations. In the event of suspicious transactions on a client's account, BITmarkets reserves the right to conduct an internal investigation, suspend, block, and/or close the client's account, and to cancel any further payments or trade positions.
 - V. Sanctions serve as a critical instrument of foreign policy, designed to promote international security, the rule of law, and adherence to international law. BITmarkets also support the objectives outlined in the United Nations Charter and the European Union Common Foreign and Security Policy. When sanctions are imposed, amended, or lifted, Bitmarkets will assess whether the client, the beneficial owner, or any individual intending to engage in a business relationship or transaction is subject to these sanctions. As part of this process, BITmarkets will determine the specific sanctions applied to the individual or entity and take appropriate actions to ensure compliance with the relevant measures.
 - VI. All documents and information received and obtained by BITmarkets will be stored, processed and maintained in strict compliance with the relevant laws and regulations aimed at preventing money laundering and terrorist financing. The use or processing of personal data for any other purposes is strictly prohibited. All documents and information received and obtained shall be stored, processed and maintained for a period of six (6) years after the end of the business relationship with the client or the date of the occasional transaction. Upon expiry of the said period, the Company shall delete personal data, unless retention for a longer period not exceeding ten (10) years is permitted or reasonably required by relevant laws or regulations.

This is a concise version of the BITmarkets AML/KYC Policy for the convenience of our clients. To obtain the full document, you may submit a request, subject to review and the validity of the purpose of the request, by sending an email to compliance@bitmarkets.com.