Anti-Money Laundering/Counter the Financing of Terrorism (AML/CFT) Policy

2023/06/20 05:45:49

Article 1 **Purposes and Basis.** In view of the fact that money laundering will undermine the development of digital asset trading, facilitate and breed corruption, pollute social morality, damage the legitimate rights and interests of Users, destroy the foundation for the sound operation of digital assets trading Platforms, increase the legal and operational risks of digital assets trading Platforms, KuCoin formulates these Rules in accordance with the User Agreement of the KuCoin Website, the User Agreement of KuCoin APP and other relevant documentation, so as to prevent money laundering and terrorist financing and fully comply with relevant regulations against money laundering and terrorist financing. By the very nature of its businesses, KuCoin will have a portfolio of clients across the globe. This international presence may trigger queries or requests for information from other law enforcement authorities. KuCoin shall therefore abide to the different laws and legal requirements imposed by the authorities in Seychelles. These rules outline the procedures to be followed in order to prevent money laundering, terrorist financing and corruption. KuCoin does not wish to be manipulated by money launderers or terrorists or to become associated with money laundering or terrorism in general. Its aim is not merely to comply with its legal obligations, but to effectively minimise the risk of exploitation by criminals. Thus, the anti-money laundering, terrorist financing and corruption policies are based on the requisite highest standards.

Article 2 **Scope of Application.** These Rules shall apply to all Users trading on the website of KuCoin and the APP thereof (hereinafter referred to as "the Platform"). The Users shall implement the provisions of these Rules in accordance with the anti-money laundering and anti-terrorist financing laws and regulations of the country or region where they are located and within the scope prescribed by the laws and regulations of the region or country

where they are located. Where there are stricter requirements in the country or region where the Users are located, such requirements shall prevail. These rules are governed by and shall be construed in accordance with the laws of Seychelles.

Article 3 **Fight Against Money Laundering and Terrorist Financing.** This refers to activities with respect to which measures have been adopted pursuant to relevant laws, relevant rules and regulations, for the purpose of preventing money laundering activities that are carried out by offenders through the Platform for the purpose of covering up and concealing the source and nature of the proceeds and profits that such offenders obtain through such crimes as those relating to narcotics, organized crimes, terrorism, smuggling, graft, bribery, financial fraud, breach of financial regulation and order, *inter alia*.

Article 4 **The Platform's Rules and Regulations against Money Laundering.** The rules and regulations of the KuCoin against money laundering (including terrorist financing; the same hereafter) include these Rules, sections concerning money laundering in the *User Agreement of KuCoin Website* and the *User Agreement of the KuCoin APP, Measures for the Management of Large-sum Transactions* and the *OTC Platform Guidelines for Users against Money Laundering and Terrorist Financing*. In the event of any conflict between these Rules and the sections on money laundering in the *User Agreement of KuCoin Website* and the *User Agreement of the KuCoin APP*, these Rules shall prevail. In the event of any conflict between these Rules and *Measures for the Management of Large-sum Transactions* and the OTC *Platform Guidelines for Users against Money Laundering and Terrorist Financing,* such measures and guidelines shall prevail.

Article 5 **Basic Principles of the Platform against Money Laundering.** The Platform monitors User risks according to the following principles:

(1) The principle of comprehensiveness. The Platform will take into account all kinds of risk factors on the basis of which Users may be suspected of money laundering, and monitor risks of all Users in an appropriate manner.

(2) The principle of prudence. On the basis of fully understanding the Users, the Platform will improve its ability to authenticate User identities, and monitor User risks in a prudent way.

(3) The principle of sustainability. The Platform will pay appropriate attention to User risks and respond to risks on the basis of actual and specific circumstances of each risk.

(4) The principle of confidentiality. User identity information, transaction information and risk level held by the Platform shall be kept strictly confidential and shall not be provided to any entity or individual unless it is required by law or regulatory authorities.

(5) The principle of hierarchical management. The Platform will regularly review the

basic information of the Users according to the risk level of each User. And the review of Users with a higher risk level shall be stricter than that of Users with a lower risk level.

Article 6 **Responsible Organ.** The Platform carries out operations against money laundering via a guidance group for money laundering affairs and a team for advancing the fight against money laundering, each of which shall consist of members from the Platform's risk control and compliance departments.

Article 7 **Functions of the Responsible Organ.** The guidance group for money laundering affairs is responsible for planning, guiding and coordinating the money laundering affairs of the Platform. Its specific responsibilities include the following:

(1) to review and approve the Platform's money laundering policies, work plans and work reports;

(2) to promulgate and update the guiding principles and rules of the Platform against money laundering;

(3) to review the Platform's and its sub-websites' organizational structure and designation of responsibilities against money laundering;

(4) to design and complete procedures for internal inspection and control of transactions;

(5) to study major and difficult problems relating to money laundering and to form solutions.

The staffing structure of the team for advancing the fight against money laundering shall be determined on the basis of regulatory requirements and location-specific conditions. The main responsibilities thereof include:

(1) to implement relevant rules against money laundering and plans of the guidance group for money laundering affairs;

(2) to implement various assignments;

(3) to analyze and identify the identity and background of any User with a suspicious transaction as well as each such suspicious transaction;

(4) to assess and adjust the risk level of Users;

(5) to conduct due diligence and continuous supervision of Users;

(6) to review and regularly examine transactions that have occurred;

(7) to report suspicious transactions to the competent authorities;

(8) to assist in the investigation at the request of any competent authority.

Article 8 **Due Diligence.** Following the principles of diligence and understanding your Users, the Platform conducts due diligence on all Users. For high-risk Users, the Platform has the right to conduct enhanced due diligence.

Article 9 **Documents Submitted by Individual Users.** As is required by the laws and regulations of different jurisdictions, the information that the Platform collects on individual Users from different countries or regions may vary. In principle, an individual User is required to provide the following information and data in accordance with relevant regulations of the Platform against money laundering:

(1) personal name;

(2) home address;

(3) date of birth;

(4) nationality;

(5) telephone number;

(6) e-mail address;

(7) a photo of the User taken within the six months from the date of registration with the Platform;

(8) photocopy of a valid Identity Card or a valid passport of the User; and

(9) other information or documents requested by the Platform.

Article 10 **Documents Submitted by Institutional Users.** As is required by the laws and regulations of different jurisdictions, the information that the Platform collects on institutional Users from different countries or regions may vary. In principle, an institutional User shall submit the following information and data in accordance with the Platform's relevant regulations against money laundering:

(1) name of the institution;

(2) registered office address of the institution;

(3) contact information of the institution;

(4) articles of association of the institution;

(5) description of the equity structure and ownership of the institution;

(6) legal representative of the institution;

(7) place of residence of the legal representative of the institution;

(8) contact information of the legal representative of the institution;

(9) the institution's business license;

(10) the institution’s consent to open an account with this Platform;

(11) letter of authorization by the institution;

(12) a copy of the valid Identity Card or a valid passport of the legal representative of the institution; and

(13) other information or documents to be provided upon request by the Platform.

Article 11 **Languages of the Submitted Documents.** The Platform only accepts documents prepared in Chinese or English. Users who submit documents prepared in any language other than Chinese or English shall engage a properly qualified translator to translate such documents into Chinese or English and have the translated version thereof properly notarized.

Article 12 **Submission of Document Copies.** Where a copy of a document is submitted, the copy shall be properly checked against the original of such document. A copy of a document may be submitted if the copy has been notarized and certified as a true and accurate copy of the original document. The certification mentioned under this Clause includes, but is not limited to, certification by an embassy, judicial certification, certification by local magistrate, or certification by a notary public.

Article 13 **Photograph-based Verification.** Users shall complete a photograph-based verification procedure as required by the Platform: the User shall have a photograph of himself/herself taken, which shows the User holding his/her identity document and a statement that the User opens his/her account with the Platform according to his/her free will. If the photograph of the User is not clear enough or fails to conform with the requirements of the Platform, the Platform shall have the right to refuse to reject the User’s registration.

Article 14 **Identification of the Beneficiary and the Controller.** The Platform has the right to identify the actual or beneficial owner or controller of the account of a User. In the case of

registration of an institutional User, the shareholder(s) holding more than 25% of the shares of the institution shall provide relevant materials and undergo identity verification according to the requirements of the Platform.

Article 15 **Identity Authentication by an Entrusted Third Party.** Where a sub-website of the Platform entrusts a third-party institution to authenticate a User's identity, the third-party institution shall meet the following requirements:

(1) the third-party institution has adopted necessary measures for User identification and storage of identity information in accordance with laws and regulations on money laundering and the Platform's relevant rules and regulations against money laundering;

(2) the third-party institution's supply of User information to the sub-website is not subject to any legal or technical obstacles;

(3) when it engages in business operation, the sub-website is able to promptly obtain the User information provided by the third-party institution and, if necessary, obtain the User's valid identity certificate, as well as the original, photocopy or photographic copies of the identity documents from the third-party institution.

Article 16 **Review of User Documents.** The Platform will verify and record the relevant information submitted by the Users in accordance with the User identification system under the Platform's relevant regulations against money laundering. If the Platform has any doubt about the information submitted by any User, it has the right to ask the User to provide other documents or consult with relevant competent authorities or departments for verification.

Article 17 **Classification of User Risk Levels.** The Platform classifies Users into three categories, i.e., low-risk Users, medium-risk Users and high-risk Users according to the materials submitted by the Users, and on the basis of such factors as the geographical location of the Users, the industries they are involved in, background of the shareholders of Users, if any, and whether Users are prominent public figures, *inter alia*. The Platform reserves the right to adjust the grading of Users.

Article 18 **Identification of High-risk Users.** High-risk Users refers to Users who comprise any of the following high-risk factors and are identified as high-risk Users after a comprehensive evaluation by the Platform. High-risk Users include:

(1) Users who have been subject to or are currently under criminal or administrative investigation, excluding Users who are investigated in connection with any civil proceeding or emergency dispute;

(2) Users who are prominent public figures, or whose controlling shareholders, actual controllers and/or actual beneficiaries are prominent public figures;

(3) Users who are from high-risk countries or regions, or their controlling shareholders, actual controllers and/or actual beneficiaries are from high-risk countries or regions;

(4) Users who are identified as key suspicious Users according to relevant procedures of the Platform;

(5) Users who are engaged in business operations in industries subject to a relatively high level of money laundering risks, such as jewelry, precious metals trading, currency exchange, pawn brokerage, money remission, nightclubs and the arms industry, etc;

(6) Users who engage in intensive trading within a certain period of time, which is seriously inconsistent with the situation on the digital assets markets; and

(7) Users who engage in unusual operations.

Article 19 **Identification of Low-risk Users.** Low-risk Users refers to those Users who are identified as low-risk Users after a comprehensive evaluation by the Platform. Low-risk factors include:

(1) Users that are financial institutions or well-known companies;

(2) Users who are natural person and of whom the Platform has proper understanding through verification and who carry a relatively low risk of money laundering;

(3) Users who are reviewed and approved by the Platform's risk control and compliance departments.

Article 20 **Identification of Medium-risk Users.** Medium-risk Users refers to Users other than those specified under Articles 18 and 19 of these Rules.

Article 21 **Adjustment of Risk Level Grading.** After the establishment of business relations with a User, the Platform will pay sustained attention to their identity and transaction status. Should there be any change or abnormality in such identity or status, or the Platform becomes suspicious about any of the information that it has by then obtained on the User, the Platform will re-identify the User identity and adjust the risk level grading of the User in a timely manner. The Platform has the discretion to adjust the User's risk level grading and may do so without providing the User with any reason.

Article 22 **Monitoring of High-risk Users.** For Users in the high-risk category, the Platform will conduct regular review to update the basic information on the Users' identity and ascertain their sources of funding, use of funds, financial standing or business status. If the Platform, on the basis of a comprehensive assessment during the regular review of a high-risk User, deems that the User and the transactions in the User's account with the Platform are normal, it may lower the risk level of such User.

Article 23 **Continuous User Identification.** Throughout the business relationship with each User, the Platform will adopt continuous User identity verification measures so as to keep following the User's transaction status, and if the Platform finds that the User's identity information or information has expired and the User fails to update such information or data within a reasonable period of time without providing any justifiable reason, the Platform will take measures to suspend the service for the User.

Article 24 **Re-identification of Users.** Under any of the following circumstances, the Platform has the right to re-identify a User's identity:

(1) where the User requests to change his/her name or designation, the type of his/her identity certificate(s) or identification documents(s), ID Card number, registered capital, business scope or legal representative;

(2) where there is any abnormality in the User's conduct or trading;

(3) where the User's name is the same as that of any criminal suspect, money launderer or terrorist financier;

(4) where the User is suspected of engaging in money-laundering or terrorist financing;

(5) where there is any inconsistency or contradiction between the information on the User that the Platform acquires and relevant information that the Platform already has in its possession;

(6) there is any doubt about the authenticity, validity and/or integrity of the User's information and materials previously obtained;

(7) other circumstances under which the Platform deems it necessary to re-identify the User's identity.

Article 25 **Trading Limits.** The Platform has the right to set and adjust at any time the maximum amount of currency that may be withdrawn for scheduled transactions, according to the transaction security and actual conditions.

Article 26 **Identification of Suspicious Transactions.** The Platform has the right to verify the following suspicious transactions and suspicious accounts:

(1) dispersed transfer-in of digital assets followed by collective transfer-out thereof within a short period of time, or collective transfer-in followed by dispersed transfer-out within a short period of time, which is clearly inconsistent with the User's identity, financing standing and/or business operation status;

(2) where an account that has been inactive for a long time is suddenly reactivated, or

(3) where a large number of accounts are opened or cancelled without any justifiable reason, and a large amount of currency is deposited or withdrawn prior to such cancellation of accounts;

(4) there is any suspicious lump-sum deposit or withdrawal in the account of an User who is a natural person;

(5) where the User engages in excessively frequent trading within a certain period of time, which is seriously inconsistent with the situation on the digital assets market; and

(6) other suspicious trading situations identified by the Platform.

Article 27 **Identification of Terrorist Financing.** If the Platform suspects that an User's transaction or attempted transaction is related to terrorism, terrorist crime, any terrorist organization, terrorist or people engaged in terrorist financing activities, it shall adopt appropriate measures, regardless of the amount of fund or value of assets involved.

Article 28 **Handling of Suspicious Conduct.** When the Platform identifies the identity of an User, it shall have the right to adopt measures such as suspending any suspicious transaction, rejecting transaction applications, reversing transactions, freezing suspicious accounts, and reporting to the competent authorities if the Platform uncovers any of the following conducts on the part of the User:

(1) the User refuses to provide valid identity certificates or other identification documents;

(2) the User refuses to update his/her profile without any justifiable reason;

(3) where, after necessary measures are adopted, the Platform still doubts the authenticity, validity and/or integrity of the User’s identity information;

(4) the User forges or alters his or her identification documents to deceive the Platform to allow it to open an account with the Platform; or

(5) the User refuses to provide a reasonable explanation for the suspicious conduct thereof, or the User’s explanation is obviously unjustifiable.

Article 29 **User Data storage system.** The Platform establishes a system for the storage of Users’ identity information and transaction records, and properly preserves documents and data such as User identity information and transaction records so as to facilitate money

laundering investigation and supervision and regulation, and prevent the loss, damage and disclosure of such information.

Article 30 **Scope of the storage of the Users' Data and Transaction Records**. User identity information and transaction data saved by the Platform includes the User identity information as provided, various data and records reflecting the User's identity identification carried out by the Platform, as well as the data and information of each transaction and other data reflecting the actual circumstances of the transactions.

Article 31 **Term for the storage of User identity information and Transaction Records.** The Platform shall keep User identity information and transaction records for specific terms depending on the following circumstances:

(1) User's identity information shall be kept for at least five years, starting from the date when the business relationship between the User and the Platform ends;

(2) transaction records shall be kept for at least five years, starting from the date when the transaction is entered into records;

(3) if the User's identity information and transaction records involve any suspicious activity that is being investigated for money laundering, and the investigation into money laundering is not completed at the expiration of the minimum storage term as is specified in the preceding paragraph, the Platform will keep them until the end of the money laundering investigation;

Article 32 **Assistance to Judicial Investigation**. If a judicial organ, law enforcement organ or other competent authority of a country or region submits a request to the Platform for assistance in connection with any investigation, the Platform shall have the right to cooperate with such investigation and provide relevant information and materials as is requested by such organ or authority, as the case may be.

Article 33 **Confidentiality in Anti-money Laundering**. Any staff member of the Platform that comes across any information relating to anti-money laundering through his or her performance of duties relating to money laundering or his or her work shall strictly comply with confidentiality requirements and keep confidential all the User identity information, suspicious transactions, terrorist financing transactions and other information that he or she may obtain. Such staff member may not provide such information to any organization, individual or any unrelated staff member of the Platform.

Article 34 **Cautions to the Users.** The Users shall pay attention to the following cautions:

(1) the Users are forbidden from lending their account details to any other person;

(2) the Users are forbidden from renting out or lending their identity certificates;

(3) the Users are forbidden from renting out, lending or disclosing important personal assets information, such as the User's account details and password;

(4) Users shall actively cooperate with the Platform in User identification.

Article 35 **Reports of Suspicious Conducts.** Users of the Platform may report to the Platform if they find that any account may be engaged in money laundering or terrorist financing activities during trading on the Platform.

Article 36 **Interpretation.** These Rules shall be interpreted by the Platform.

Article 37 **Effective Date.** These Rules shall come into effect on the date of promulgation thereof.

Privacy Policy
Risk Disclosure Statement
AML & CFT
Law Enforcement Requests
Whistleblower Contact

Trading Fee
Referral
GemSPACE
KuCoin Learn
Converter

Service

Beginner's Guide
Help Center
Submit a Ticket
Technical Support
Bug Bounty
Ticket Verification
Official Verification Center
Fees & VIP
Safeguard Program
Special Treatment
Delisting
Sitemap

Business

Affiliate Program
Brokers
Institutions
API Services
Token Listing
P2P Merchant Application

Crypto Prices

Bitcoin (BTC) Price
Ethereum (ETH) Price
Ripple (XRP) Price
KuCoin Token (KCS) Price
More Prices

Learn

Buy Solana
Buy XRP
Buy Monero
Buy Hyperliquid
Buy SUI
Buy Aptos Network
Buy Cardano
Buy Pepe

Developer

API Documentation

SDK

Download Historical Data

Partners

Kolo Wallet

App Download

Android Download

iOS Download

Community

08:35:45 (UTC+8)

24h Volume