

# COTX KYC Policy - Know Your Customer

## Terms

KYC: Know Your Customer

AML: Anti-Money Laundering

CTF/TF: Counter-Terrorism Financing

PEP: Politically Exposed Persons

UBO: Ultimate Beneficial Owner

## Know Your Customer

COTX will strive to identify the risk it faces that its products and services are amenable to use for illegal financing activities or by persons, entities, or organizations, or in support of transactions in countries with which transactions are prohibited by law or COTX' policy.

COTX will conduct a risk-based assessment of its products and services, focusing on the likelihood that its products and services are amenable to use to commit illegal financing activities. This risk-based assessment will consider factors such as the customer background, customer onboarding processes for customers who are in face-to-face contact with COTX employees, as well as customers who sign up for products and services remotely; the geographic location of its customer base and the countries and regions in which the customers operate and transact business; and the delivery channel for its products and services; customer's behavior when the customer use COTX products and services.

## COTX KYC Practices

**A.** For all Helium/DeWi related COTX products and service, COTX and COTX customers must follow Helium/DeWi's business conduct and principles. COTX will strive to quantify the financing risk level of each customer. COTX will also seek to understand the normal business activities of customers. COTX KYC will evaluate customers based on the following criteria:

(1) **Background of customers** – Customers with high-profile positions, such as public institutions or Politically-Exposed Persons, having high-volume transactions with COTX will have a higher risk than a small business with fewer transactions.

(2) **Country of origin and operation** – COTX seeks to serve customers around the world; however, customers who come from or operate or transact business in

jurisdictions with lower standards regarding illegal financing programs or with unstable political environments may be of higher risk than customers from countries with more stringent AML/CTF requirements or stable governments.

(3) **Business or Profession** – COTX uses 3rd party KYC services to identify potential higher-risk businesses and professions. COTX will also identify higher-risk customers from a money laundering and terrorist financing perspective for use during the onboarding process. Higher-risk customers may only become customers following enhanced due diligence during the customer onboarding process. Certain customer types are unacceptable and cannot be signed up for services or place purchasing orders regardless of any enhanced due diligence.

**B.** COTX will take reasonable steps to determine the true identity of all customers and beneficial owners of customers.

(1) As soon as practicable after the first contact between COTX and a potential customer, COTX will collect evidence of and verify the identity of the customer or, in the case of an entity, the primary beneficial owners of the customer. COTX will undertake appropriate due diligence measures for applicants who are not signed in a face-to-face acquisition transaction that are no less stringent than those measures used in face-to-face customer acquisition transactions. As used in this context, “primary beneficial owner” means beneficial owners of 25% or more of equity interests in the customer entity, as well as any person with significant responsibility to control, manage or direct the customer entity.

(2) In general, evidence of a customer’s identity will be sufficient if it is reasonably capable of establishing that the applicant is the person they claim to be. COTX is satisfied that the evidence does show that fact by the procedures maintained according to this KYC policy. To the extent practicable, customer identification rely on trusted third-party identity verification tools or official documents issued by a government agency or other similar documents that are hard to obtain illicitly and counterfeit.

(3) Although many jurisdictions impose specific requirements for obtaining and verifying documentation, in the absence of such specific needs, the basic procedures for verifying the identity of an individual or business may include an electronic identity verification process as outlined in the relevant jurisdiction’s KYC Policy or customer onboarding processes or, if the applicant fails such electronic process or the electronic process is not available, obtaining information that would establish and confirm the customer’s identity before initiating the contract relationship, such as Name, home address, Social Security number, and address of the customer’s officers, directors, principals, beneficial owners, or agents (collectively, the “customer’s principals”);

(4) Those customers who are identified as representing a higher risk of money laundering or terrorist financing – either because of their industry, location, countries of business activities or background – will be subjected to enhanced due diligence techniques. Such enhanced due diligence techniques may include checks of third-party credit or public record databases, actual site visits, copies of accountant-prepared financial statements, copies of business leases, and other evidence of the customer’s actual existence and legal/ethical compliance that independent sources can corroborate. If during the course of the customer identification and verification process “Red Flags” or reasons for suspicion about the customer’s identity arise, COTX will apply enhanced due diligence procedures. The customer may need to provide more documents and evidence to pass through enhanced due diligence.

(5) During our relationship with a customer, COTX will carry out a regular review of existing records to ensure that identity documents remain up-to-date and relevant. At a minimum, a review should be conducted if the customer has engaged or may have engaged in any suspicious activities; COTX becomes aware of a material change to the customer or to its customer relationship with COTX; or COTX has actual knowledge of the previously validated records have expired or have become invalid; or COTX received notification from 3rd party about a customer may have suspicious or wrongfully activities, i.e., violate Helium/DeWi rules.

Reference. Helium/DeWi's requirement about "Gaming activities" and COTX's responsibility to report and punish these gaming users/distributors:

<https://cotx-store.com/pages/cotx-store-terms-of-service>

Section: Miner Makers and Distributors' responsibility to protect Helium network and anti "Gaming" Policy

**C.** COTX will obtain information from its customers to identify the purpose and intended nature of the business relationship. As part of the COTX’s business processes, COTX shall get information from the customer regarding the customer’s business to understand the customer’s potential transaction volume, anticipated types of transactions, and other information regarding the business relationship. Understanding this information will help the COTX identify potentially suspicious transactions. Such information will be kept in the customer’s file for future reference. If, while obtaining information about the customer’s business and anticipated transactions, “Red Flags”, or reasons for suspicion arise, COTX will apply enhanced due diligence procedures.

#### **D. Prohibited Countries**

As a matter of COTX policy, considering the combined effect of legal requirements in jurisdictions in which COTX may operate, and based on global risk considerations, COTX will not accept customers in or participate in transactions involving the countries embargoed by Singapore, China. Please check the list: <https://cotx-store.com/pages/cotx-shipment-policy>

#### **E. Restricted Persons or Entities – Primary Beneficial Owners**

COTX will screen all customers' or potential customers' names and addresses and the names and addresses of all customers or potential customers' primary beneficial owners against regional sanctions lists of prohibited individuals and organizations. As

used in this context, "primary beneficial owner" means beneficial owners of 25% or more of equity interests in the customer entity, as well as any person with significant responsibility to control, manage or direct the customer entity. The regional sanctions lists against which COTX will screen customers will, at a minimum, be the China, Singapore, and United States' sanction lists. We will refer hereafter to the collective lists against which COTX will screen as the "Restricted Parties List."

The Restricted Parties List must be checked at the following times:

- During customer acquisition;
- Periodically during the reviews of customer records and identity documents;
- In the event, COTX suspects a customer is engaged in a high-volume or suspicious transaction; or
- Whenever COTX becomes aware of any change to the relevant list or any customer or customer's principal information.
- Whenever COTX receives notification from MOC/DeWi/Helium.

Whenever COTX discovers that the customer or potential customer name or address or any of the customers or potential customers principals' names or addresses may match a person or entity or name and address on the Restricted Parties List or operate in a prohibited country, COTX shall, in the case of a current customer, immediately suspend the customer's contract, or, in the case of a potential customer, refuse to approve the customer for services, and shall notify the DeWi/Helium/COTX senior management/COTX stakeholders/related jurisdictions. Then, COTX will initiate the investigation process and report to associated jurisdictions. The investigation, its results, and subsequent notifications or decisions not to notify must be retained for at least five (5) years.

Reference. United Nations Security Council Consolidated List  
<https://www.un.org/securitycouncil/content/un-sc-consolidated-list>

## **F. Politically Exposed Persons**

Individuals who have or have had positions of public trust such as government officials, senior executives of government corporations, politicians, important political party officials, etc. and their families and close associates, also known as "Politically Exposed Persons," require enhanced due diligence at boarding and during the customer relationship. During the customer acquisition process, COTX will inquire as to whether a customer or principal is a Politically Exposed Person. In addition to normal due diligence methods for its customers, if a customer or principal is a Politically Exposed Person, COTX must obtain approval from senior management for establishing a business relationship with such person, take reasonable measures to establish the source of wealth and source of funds for such person, and conduct enhanced ongoing monitoring of the business relationship.

**G.** When a customer's true identity cannot be determined, COTX will not provide products or services to the customer. COTX will never knowingly establish a business relationship with a customer who provides a fictitious name or insists on anonymity. COTX will not enter into a business relationship with a customer for whom it cannot sufficiently verify the identity of the customer or the beneficial owners.

**H.** Under certain circumstances, based on the risks presented by a business partner or a customer, COTX will terminate a relationship. COTX reserves the right to close customer and other business relationships based on the risk of money laundering or terrorist financing a customer or other relationship partner represents, or MOC/DeWi/Helium's instruction or notification of the customer's misconduct. Such risks may be discovered at any time during the relationship, including, but not limited to, (1) when a customer account or business relationship has been established and subsequently an issue arises with the customer's identity verification information; (2) where information is discovered to be incorrect or fraudulent or for other related reasons; (3) new facts arise regarding the customer or business partner that indicate that the relationship involves a higher level of risk than COTX is willing to undertake; and (4) a customer's suspicious conduct indicates that the relationship should not be maintained.

## **Monitoring Customer Activities**

COTX will monitor customer activity to detect and report high-value or suspicious activities. COTX employees should be aware of customer transactions and report any suspicious activities or transactions. COTX will exercise ongoing due

diligence for the business relationships it has with every customer by examining customer transactions to help ensure they are consistent with COTX's knowledge of the customer, its business, and risk profile.

## **KYC Record Protection and Retention**

COTX will comply with the specific record retention requirements imposed by the jurisdictions in which it operates. All customer submitted KYC data and documents would be transmitted/stored/managed under security protection (i.e., TLS, AES encryption, MFA). Only authorized COTX employees could access these data, and we only use qualified 3rd party tools to conduct customer due diligence. Suppose a customer's business relationship with COTX ended. In that case, we will archive/remove all KYC information permanently based on the customer's requirements, except for the business records, which we have to archive for audit based on the law/regulation requirements.

## **Policy Changes**

We may change our KYC Policy from time to time to comply with the laws, regulations, and Helium/DeWi requirements. And COTX won't notify a customer about these changes, and the customer must check COTX websites by themselves.