
# KNOW YOUR CUSTOMER STANDARDS

**KYC Standards**

KNOW YOUR CUSTOMER (KYC) POLICY, ON BOARDING OF CUSTOMER, PREVENTION OF MONEY LAUNDERING & RISK CATEGORISATION

**I THE BACKGROUND:**

The Master Direction issued is mainly in respect of 'Know Your Customer' (KYC) Guidelines and Anti Money Laundering Standards (AML) based on 'Prevention of Money Laundering Act, (PMLA) and rules thereunder, the recommendations made by the Financial Action Task Force (FATF) on anti-money laundering standards and amendments made in the PMLA, from time to time. These Directions lay down the minimum requirements / disclosures to be made in respect of clients.

**II OBJECTIVE:**

-> This Policy shall be treated as internal guidelines for customer acceptance, KYC and AML- PMLA activities undertaken by Cipher Crypto Technologies Ltd. (Cipher). The objective of this policy is to prevent the Cipher from being used, intentionally or unintentionally, by criminal elements for money-laundering activities, KYC procedures enable the Cipher to know/understand their customers and their financial dealings in better way which in turn helps manage the risks prudently.

-> To put in place systems and procedures for customer identification and verifying his/her identity and residential address.

-> To monitor transactions of a suspicious nature.

-> The policy will be disseminated to all employees at all levels in the organization who deal/handle account information, financial transactions, money and customer records etc. relating to the clients.

**III Customer Acceptance Policy (CAP)**

The following Customer Acceptance Policy indicates the criteria for acceptance of customers

1. No account shall be opened in anonymous or fictitious name(s).

2. No Minors. Eligible age is above 18 years.

3. No one above the age of 75 years.

4. No Societies.

5. Only Legal individual can open account with Cipher.

6. Account to be opened through web or mobile application ONLY.

7. No walk ins.

8. One customer ONLY one account.

9. Enhanced documents may be sought by Cipher based on the velocity of customers from time to time.

**V Due Diligence from PMLA Point of view:**

1. Customer due diligence ("CDD") measures shall be applied to an extent that is sensitive to the risk of money laundering and terrorists financing depending on the type of customer, business relationship or transactions involved.

2. Cipher shall determine from available sources of information whether the client or potential client is a politically exposed person.

3. Documents required, and other information will be collected from clients as mentioned below. Any additional documents or due diligence can be carried out Cipher depending upon perceived risk. Below is the indicative list of documents to be collected from the client.

**KYC documents-**

Types of Entity

Documents required

**Individual/Proprietor**

1. National ID card with photo on it.
2. Address Proof document.

**Corporate**

1. Certificate of Incorporation

2. Memorandum & Articles of Association

3. Board Resolution for Trading in cryptocurrency using corporate account at Cipher

4. National ID of Authorized person

5. Government approved ID proof of any one of the directors

6. Address proof of company

7. Address Proof of authorized person

**Partnership Firm**

1. Certificate of Registration (for registered partnership firms only)

2. Partnership Deed

3. Authorization Letter for trading/investment in Cipher

4. National ID of Authorized person

5. Address proof of firm

6. Address Proof of authorized person

Note- Apart from these above documents Cipher reserves the right to call for additional documents for further verification based on customer volume and monitoring pattern.

4. In case of corporate, the antecedents of the company (change of name and registered office in particular) and of all promoters and directors will be traced.

5. An assessment shall be made of the financial worthiness of the client by obtaining appropriate declarations at KYC stage.

6. A thorough assessment shall be carried out to ascertain whether the client is dealing with the company on his own behalf or someone else is the beneficial owner. If there doubts, before acceptance of the clients, thorough due diligence shall be carried out to establish the genuineness of the clients. Secrecy laws shall not be allowed as a reason to disclose true identity of the beneficiary/transacting party.

7. No account shall be opened in a fictitious name or on an anonymous basis.

8. No client shall be accepted where it is not possible to ascertain the identity of the client, or the information provided is suspected to be non-genuine, or if there is perceived non-cooperation of the client in providing full and complete information. Cipher shall not continue to do business with such a person and file a suspicious activity report. Cipher shall consult the relevant authorities in determining what action it shall take when it suspects suspicious transactions being carried out.

9. No transaction or account-based relationship is to be undertaken without following the Client Due Diligence Process.

10. Any transaction from the client shall be accepted only after KYC and banking details of the customer are accepted by Cipher and procedure is completed.

**VI CLIENT RISK CATEGORIZATION:**

1. Based on the various factors and risk parameters, the clients shall be categorized into High, medium and low risk category.

2. Certain clients may be of a higher or lower risk category depending on the circumstances such as the client's background, type of business relationship or transaction, etc. The illustrative factors for risk profiling is given as under (list is indicative and can be expanded as per business requirements and experience):

I. Geographical Location and Category of client.

II. Nature of Business activity

III. Financial Health vs Trade Volume

**IV. Income Range**

3. The authority to enter in to financial transactions on behalf of a corporate customer (private/public limited company) shall be backed by a resolution of the Board of Directors. In case of a partner entering into a financial transaction on behalf of a partnership firm, the LOA or POA shall be signed by all the remaining partners of the firm. In case of a Trust or a Foundation, such an authority shall be backed by a resolution passed by the Board of Trustees or Managing Board as the case may be.

4. Client identification process shall be carried out at following different stages:

I. While establishing the relationship with the client.

II. While carrying out transactions for the client

III. When the Cipher has doubts regarding the veracity or the adequacy of previously obtained client identification data.

5. Failure/Refusal by prospective client to provide satisfactory evidence of identity shall be noted and reported to the higher authority within the organization.

6. Risk based Monitoring approach shall be followed. Broad categories of monitoring and reason for suspicion and examples of suspicious transactions for Cipher are indicated as under:

1. Identity of Client

a) False identification documents

b) Identification documents which could not be verified within reasonable time.

C) Doubt over the real beneficiary of the account.

d) Accounts opened with names very close to other established business entities

2. Suspicious Background

a) Suspicious background or links with known criminals

3. Multiple Accounts

a) Large number of accounts having a common account holder or authorized signatory with no rationale.

b) Unexplained transfers between multiple accounts with no rationale

4. Activity in Accounts

a) Unusual activity compared to past transactions

b) Sudden activity in dormant accounts

c) Activity inconsistent with what would be expected from declared business

5. Nature of Transactions

a) Unusual or unjustified complexity

b) No economic rationale or bonafide purpose

c) Source of funds/Cryptocurrencies are doubtful

6. Value of Transactions

a) Value just under the reporting threshold amount in an apparent attempt to avoid reporting

b) Inconsistent with the clients apparent financial standing

c) Inconsistency in the transactions pattern by Customers.

7. Cipher will ensure that information sought from the customer is relevant to the perceived risk, is not intrusive, and is in conformity with the guidelines issued in this regard. Any other information from the customer will be sought separately with the client's consent and after opening the account.

**VII. EXCEPTION HANDLING:**

Exceptions to this Policy must be approved by the Chief Compliance Officer, or a designated person. All exceptions must be documented, with reasons for the exceptions, including expiration or review date and, wherever necessary, include an action plan and timelines for compliance with the policy.

**VIII. KYC REJECTION PROCEDURES:**

In case where the documents or information obtained from client is not sufficient as outlined in the policy, the KYC will be rejected unless it is covered under the exception handling procedure as mentioned in clause above. Any changes/amendments made in the Policy shall be put before the Board of Directors in their meeting immediately succeeding such changes/amendments, for purpose of information.

**IX. EFFECTIVE DATE AND REVIEW:**

The policy would be reviewed in line with review requirements of the Cipher or as and when considered necessary by Chief Compliance Officer and/or Board of Directors but not later than once a year.