

# Anti-Money Laundering (AML) Policy

## 1. PURPOSE

CoinMENA (licensed by The Virtual Assets Regulatory Authority (VARA) as COINMENA FZE) has been established in the Emirate of Dubai as a virtual asset service provider. CoinMENA is a private Emirati Shareholding closed joint-stock company. Please take the time to read this Privacy Policy carefully. If you have any questions about this Privacy Notice, please get in touch with our support team.

## 2. POLICY STATEMENT

The company's policy prohibits and actively prevents money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities by complying with all applicable requirements under the The Virtual Assets Regulatory Authority (VARA) and its implementing regulations. The company mandates all its representatives to comply with its AML policy while being engaged in performing operations of the company irrespective of its operating jurisdictions.

## 3. AML POLICY PROGRAMME

The AML policy program of the company comprises key measures that ensure compliance with regulatory directives. These measures are:

- AML Policy - Develop, document, and implement the company's AML policy and procedures, reviewed and approved by the company's board on an annual basis at the minimum.
- Compliance Officer & MLRO - The company shall appoint a Compliance Officer & MLRO responsible for coordinating and overseeing the AML compliance program on a day to day basis.
- Customer Acceptance - The company has documented a detailed procedure to control the eligible applicants' acceptance as its customers. These procedures comply with the relevant guidelines of the VARA and observe globally recognized best practices.
- Transaction Oversight - Develop, document, and implement written procedures to prevent, detect, and report suspicious transactions internally and externally as mandated under the AML policy.
- Training - Providing AML training periodically to all the relevant employees.
- Independent Review - The company shall appoint, subject to approval from the VARA, a competent, separate entity to conduct an AML Policy program's annual assessment.

## 4. RISK-BASED APPROACH

The company shall implement a risk-based approach to identify, assess and understand the (ML/TF) risks to which it is exposed and take the necessary AML and Counter Financing of Terrorism (CFT) control measures to mitigate them. During this, the company shall assess, identify and understand the ML and TF risks concerning its customers, their respective geographies, the company's own operating jurisdictions, and its products, services, transactions, and distribution channels (collectively referred to as "Operations").

## 5. COMPLIANCE OFFICER & MLRO

The company shall appoint, subject to CBB approval, a Compliance Officer & Money Laundering Reporting Officer (MLRO) to oversee the implementation of its AML Policy program. The incumbent shall be a member of the company's senior management and report to the Board of the company. Among others, his responsibilities shall include being the single point of contact for the CBB in matters related to AML, regulatory filings, reporting relevant transactions, and ensuring compliance with applicable laws.

The roles of Compliance Officer & MLRO may be assigned to a single individual subject to regulatory approval and in proportion to the company's operations' volume and complexities.

## 6. CUSTOMER ACCEPTANCE

The company shall accept applicants as its customers only after completing its due diligence procedures established in compliance with the The Virtual Assets Regulatory Authority (VARA)'s relevant directives. For onboarding of natural persons, the company shall obtain and record the below-mentioned information and verify the same against pertinent valid documents (including but not limited to Passport, Residency Visa, Bank Statement, Utility Bill, etc.) submitted by the applicant as required by the procedures of the company.

- Full legal name and any other names used;
- Full permanent address (i.e., the residential address of the customer; a post office box is insufficient);
- Date and place of birth;
- Nationality;
- Passport number (if the customer is a passport holder);
- CPR or Iqama number (for residents of Bahrain or GCC states);
- Telephone/fax number and email address (where applicable);
- Occupation or public position held (where applicable);
- Employer's name and address (if self-employed, the nature of the self-employment);
- Type of account, and nature and volume of anticipated business

- Past, current, and prospective dealings with the Company;
- Signature of the customer(s);
- Source of funds; and
- Source of Securities.

For onboarding, legal persons, the company shall implement procedures to obtain and record:

- The entity's full name and other trading names used;
- Registration number (or equivalent);
- Legal form status;
- Registered address and the trading address (including a branch where applicable);
- Objectives and type of business activity;
- Date and place of incorporation or establishment;
- Telephone, fax number, and email address;
- Regulatory body or listing body (for regulated activities such as financial services and listed companies);
- Name of external auditor (where applicable);
- Type of account, and nature and volume of anticipated business dealings with the Company;
- Source of funds

Information records shall also be verified against appropriate documentation including but not limited to Trade License, Certificate of Incorporation, MOA & AOA, Board Resolution, Passport of each major shareholder, and authorized representative to the account.

The company shall conduct enhanced due diligence for relevant applicants that it may deem necessary according to its internal procedures or comply with the regulatory requirements. All records on the onboarding of a customer and his respective transactions shall be maintained by the company for not less than ten years from the date of termination of the relationship unless otherwise advised by the VARA.

## 7. TRANSACTION OVERSIGHT

The company mandates its MLRO to maintain oversight over its customers' transactions and document inconsistencies observed (if any) against the customers' expected behavior. MLRO shall also review all internal reports filed by the company's employees or alerts generated by the company's automated systems to investigate any unusual customer activity patterns.

MLRO shall ensure that all suspicious transactions are documented and reported to the appropriate regulatory body with the necessary documentation. The company shall maintain a record of all internal and external reports for five years from the date of reporting unless otherwise directed by the VARA or any other appropriate regulatory body.

## 8. TRAINING

The MLRO of the company shall ensure to undertake training sessions for each employee of the company that is directly or indirectly related to the customer transactions or services of the company. Such training shall include knowledge of the company's products and services, ML & TF typologies associated with it, and guidelines for identification & reporting relevant transactions internally and externally.

This training shall be provided upon induction to each new employee and at least once a year for all existing ones. MLRO shall also arrange appropriate training sessions at least once a year for the board of directors to ensure that they are well apprised of the AML measures and any other relevant matter.

## 9. INDEPENDENT REVIEW

The company shall arrange for an independent assessment of the company's program by an external entity. Such an entity may be the External Auditor or any other competent agency, subject to the approval of VARA. This review shall cover independent testing of the company's internal controls against a sample of data selected randomly and identify gaps or control failures. The findings of such assessment shall be shared with the Board and the VARA.