

Anti-Money Laundering (AML) Policy

Aeon Funded L.L.C-FZ

Meydan Grandstand, SHARED DESK 6th floor
Meydan Road
Nad Al Sheba
Dubai, United Arab Emirates

1. Introduction

Aeon Funded is committed to preventing money laundering and terrorist financing activities. This Anti-Money Laundering (AML) Policy outlines our procedures to ensure compliance with international AML regulations and best practices.

2. Know Your Customer (KYC) and Customer Due Diligence (CDD)

- We verify the identity of all customers before allowing them to engage in transactions.
- Customers must provide valid identification, proof of address, and any additional information required for risk assessment.
- Enhanced Due Diligence (EDD) is required for high-risk customers, such as politically exposed persons (PEPs) or those from high-risk jurisdictions.
- Periodic reviews are conducted to ensure the continued accuracy of customer information.

3. Monitoring Transactions and Risk Mitigation

- Aeon Funded employs automated and manual monitoring to detect suspicious activities, including:
 - Unusually large transactions.
 - Rapid movement of funds between accounts.
 - Transactions involving high-risk jurisdictions or sanctioned individuals/entities.
- Any suspicious transactions will be reviewed, documented, and escalated to the relevant authorities when necessary.

- We implement risk-based approaches to mitigate potential threats and ensure compliance with international AML guidelines.

4. Restricted Jurisdictions

To comply with international regulatory standards, Aeon Funded does not engage in business with individuals or entities located in the following restricted jurisdictions:

- **Iran**
- **Myanmar**
- **Russian Federation**
- **Belarus**
- **North Korea**
- **Cuba**
- **Syria**
- **Sudan**
- **South Sudan**
- **Venezuela**
- **Crimea (Ukraine region)**
- **Afghanistan**
- **Yemen**
- **Democratic Republic of the Congo**
- **Central African Republic**
- **Lebanon**

These jurisdictions are considered high-risk for money laundering and terrorist financing activities.

5. Compliance with International Sanctions

- Aeon Funded adheres to the sanctions imposed by organizations such as:
 - The United Nations (UN)
 - The Office of Foreign Assets Control (OFAC)
 - The European Union (EU)
 - The Financial Action Task Force (FATF)
- Any individuals or entities listed on sanction lists will be prohibited from engaging in business with Aeon Funded.

6. Record Keeping

- We maintain records of customer identification, transactions, and communications for a minimum of five (5) years.
- Records will be made available to regulatory authorities upon request.
- All customer interactions and due diligence processes are securely stored to ensure compliance and transparency.

7. Reporting Suspicious Activities

- Any employee suspecting a transaction is linked to money laundering or terrorist financing must immediately report it to the Compliance Officer.
- Aeon Funded will submit Suspicious Activity Reports (SARs) to the relevant regulatory bodies as required by law.
- No customer or third party will be informed when a report is made to avoid tipping-off violations.

8. Employee Training and Awareness

- All employees receive regular training on AML regulations and their responsibilities in preventing money laundering.
- Training includes:
 - Recognizing suspicious activities.
 - Proper reporting procedures.
 - Updates on AML laws and regulatory changes.
- Employees are required to complete refresher training annually.

9. Policy Review and Updates

- This AML policy is reviewed periodically to ensure alignment with evolving regulatory standards.
- Updates may be implemented based on:
 - Changes in international AML laws and guidelines.
 - Internal audits and risk assessments.
 - Recommendations from regulatory authorities or compliance experts.
- The Compliance Officer is responsible for ensuring that any updates are effectively communicated and implemented.

10. Conclusion

We are committed to maintaining a secure and compliant financial environment. Any violation of this policy may result in termination of services, legal action, and reporting to regulatory authorities as required by law.