UEXO

Beyond Boundaries

ANTI-MONEY LAUNDERING & COUNTERING THE FINANCING OF TERRORISM POLICY

(AML / CFT POLICY)

1. INTRODUCTION

UEXO Global Ltd. (the "Company") has a Global Business Licence registered in the Republic of Mauritius under registration number 179291 and is licensed and authorised by the Mauritius Financial Services Commission ("FSC") under Licence Number GB21026300.

The registered office of UEXO Global Ltd is 12th Floor, Hennessy Court, Pope Hennessy Street, Port Louis, Mauritius 72201.

UXO Services Ltd. is incorporated in the Republic of Cyprus under registration number HE437025 and has its registered office at Archiepiskopou Makariou III, 84, Office 1, 6017, Larnaca, Cyprus. UXO Services Ltd. acts as a non-regulated group services company providing administrative, operational and technical support to UEXO Global Ltd.

This Anti-Money Laundering and Countering the Financing of Terrorism Policy ("Policy") sets out the internal framework adopted by UEXO Global Ltd. (the "Company") to prevent, detect, mitigate and report money laundering, terrorist financing, proliferation financing and other financial crime risks in accordance with:

- The Financial Intelligence and Anti-Money Laundering Act 2002 (Mauritius)
- The Financial Intelligence and Anti-Money Laundering Regulations
- FSC Mauritius Rules and Codes
- Applicable United Nations sanctions frameworks
- FATF Recommendations
- Any other applicable laws and regulatory guidance

This Policy applies to all directors, senior management, employees, officers, contractors and service providers acting on behalf of the Company.

2. PURPOSE

The purpose of this Policy is to:

- Prevent the Company from being used for money laundering, terrorist financing or other financial crime;
- Ensure compliance with FSC Mauritius regulatory obligations;
- Establish a risk-based framework for customer due diligence (CDD), enhanced due diligence (EDD), transaction monitoring and reporting;
- Protect the integrity and reputation of the Company;

- Align operational controls with the Client Agreement and onboarding framework.

3. RISK-BASED APPROACH

The Company adopts a risk-based approach (“RBA”) to AML/CFT compliance.

Risk assessment is conducted at:

- Customer level
- Product level
- Channel level
- Geographic level
- Counterparty level

Clients are categorised into risk tiers (Low, Medium, High) based on:

- Country of residence / incorporation
- Source of funds
- Occupation / business activity
- Transaction behaviour
- Use of third-party payment methods
- PEP or sanctions exposure
- Corporate ownership complexity

Higher-risk clients are subject to enhanced due diligence and ongoing monitoring.

The Company reserves the right to refuse onboarding or terminate business relationships where AML risk cannot be satisfactorily mitigated.

4. CUSTOMER DUE DILIGENCE (CDD)

The Company shall identify and verify the identity of all clients prior to establishing a business relationship.

4.1 Natural Persons

The following minimum documentation is required:

- Valid government-issued identification
- Proof of residential address
- Self-declaration of source of funds
- Screening against sanctions and PEP databases

4.2 Legal Persons

The following shall be obtained:

- Certificate of incorporation
- Memorandum and Articles of Association
- Register of Directors
- Register of Shareholders
- Identification of Ultimate Beneficial Owners (UBOs)
- Proof of business address
- Nature of business activity
- Source of funds and expected trading activity

UBOs holding 10% or more ownership or control shall be identified and verified.

5. ENHANCED DUE DILIGENCE (EDD)

EDD shall apply where:

- The client is a Politically Exposed Person (PEP)
- The client is resident in a high-risk jurisdiction
- Complex ownership structures exist
- Large or unusual transactions occur
- There is suspicion of financial crime
- The client uses cryptocurrency funding methods

EDD measures may include:

- Senior Management approval prior to onboarding
- Verification of source of wealth
- Additional documentation
- Independent verification of beneficial ownership
- Increased transaction monitoring

The Company may reject or exit any client where risk cannot be mitigated to acceptable levels.

6. ONGOING MONITORING

The Company shall conduct ongoing monitoring throughout the business relationship.

This includes:

- Monitoring trading patterns for unusual behaviour
- Monitoring deposit and withdrawal activity
- Monitoring use of third-party payments
- Screening against updated sanctions and PEP lists
- Periodic KYC refresh
- Review of expired documentation

Where documents expire, clients may be restricted from trading or withdrawing until updated documents are provided.

7. SANCTIONS COMPLIANCE

The Company prohibits business with individuals or entities subject to sanctions imposed by:

- United Nations
- European Union
- United Kingdom
- United States OFAC
- Mauritius authorities

All clients are screened at onboarding and periodically thereafter.

If a sanctions match is identified:

- The account shall be frozen immediately
- Internal escalation shall occur
- Regulatory reporting obligations shall be fulfilled

8. CRYPTOCURRENCY FUNDING

Where cryptocurrency funding is permitted:

- Clients must declare wallet ownership
- The Company may require proof of wallet ownership
- Blockchain analytics tools may be used
- High-risk wallet addresses may be rejected
- Third-party wallet funding is prohibited

The Company reserves discretion to refuse crypto deposits where AML risk is identified.

9. SUSPICIOUS TRANSACTION REPORTING (STR)

Any employee who suspects money laundering or terrorist financing must immediately report it internally to the designated MLRO.

Indicators may include:

- Structuring of transactions
- Sudden large deposits inconsistent with profile
- Rapid deposit and withdrawal cycles
- Refusal to provide documentation
- Use of third-party payment methods
- Abnormal trading inconsistent with declared knowledge

The MLRO shall determine whether a Suspicious Transaction Report (STR) must be filed with the Mauritius Financial Intelligence Unit (FIU).

Tipping-off is strictly prohibited.

10. RECORD KEEPING

The Company shall maintain records for a minimum of seven (7) years or as required by law.

Records include:

- Identification documents
- Risk assessments
- Transaction history
- Internal investigation notes
- STR filings
- Communications related to AML reviews

Records must be retrievable without undue delay.

11. INTERNAL CONTROLS

The Company shall implement:

- Segregation of duties
- Controlled system access
- Audit trails within CRM systems
- Periodic internal compliance reviews
- Independent audit where required

Failure to adhere to AML procedures may result in disciplinary action.

12. GOVERNANCE & RESPONSIBILITY

Senior Management is responsible for ensuring:

- AML framework effectiveness
- Adequate staffing and resourcing
- Independent oversight
- Periodic review of this Policy

An appointed MLRO shall:

- Oversee AML implementation
- Escalate suspicious matters
- Report to regulators where required
- Maintain AML training standards

13. TRAINING

All relevant employees shall receive AML training upon onboarding and periodically thereafter.

Training shall cover:

- Red flags
- Sanctions compliance
- Reporting obligations
- Internal escalation procedures
- Updates in regulatory requirements

14. BREACHES & ENFORCEMENT

Where AML breaches occur:

- Immediate containment measures shall be applied
- Root cause analysis shall be conducted
- Remediation steps shall be documented
- Regulatory disclosure shall be made where required

The Company reserves the right to terminate relationships and freeze accounts where AML risk is identified.