

# ANTI-MONEY LAUNDERING (AML) & KNOW YOUR CUSTOMER (KYC) POLICY

UEXO LLC is a limited liability company incorporated and registered in Saint Vincent and the Grenadines under the Limited Liability Companies Act, with Formation No. 3574 LLC 2024. The registered office address is Euro House, Richmond Hill Road, Kingstown, Saint Vincent and the Grenadines.

## 1. PURPOSE, SCOPE AND REGULATORY ALIGNMENT

### 1.1 Purpose

1.1.1 This Anti-Money Laundering (“AML”) and Know Your Customer (“KYC”) Policy (the “Policy”) establishes the framework by which UEXO LLC (the “Company”):

- (a) prevents, detects and reports money laundering and terrorist financing;
- (b) ensures compliance with applicable legal and regulatory obligations;
- (c) protects the integrity of its operations and financial system.

### 1.2 Scope

1.2.1 This Policy applies to:

- (a) all clients (individual and corporate);
- (b) all employees and officers;
- (c) all onboarding, transactional and ongoing monitoring activities.

### 1.3 Regulatory Alignment

1.3.1 This Policy is aligned with:

- (a) Financial Action Task Force (FATF) Recommendations;
- (b) international AML best practices;
- (c) risk-based approach principles.

## 2. GOVERNANCE AND OVERSIGHT

### 2.1 AML GOVERNANCE STRUCTURE

2.1.1 The Company shall establish an AML governance framework consisting of:

- (a) Compliance Function;
- (b) AML Officer / MLRO (Money Laundering Reporting Officer);
- (c) Senior Management oversight.

## **2.2 MLRO RESPONSIBILITIES**

2.2.1 The MLRO shall be responsible for:

- (a) oversight of AML controls;
- (b) review of suspicious activity;
- (c) reporting obligations;
- (d) maintaining AML records.

## **2.3 THREE LINES OF DEFENCE**

2.3.1 AML controls shall operate under:

- (a) First Line: onboarding and operations teams;
- (b) Second Line: compliance monitoring;
- (c) Third Line: independent review / audit.

## **3. RISK-BASED APPROACH**

### **3.1 CLIENT RISK CLASSIFICATION**

3.1.1 Clients shall be classified as:

- (a) Low Risk (SDD – Simplified Due Diligence);
- (b) Medium Risk (CDD – Standard Due Diligence);
- (c) High Risk (EDD – Enhanced Due Diligence);
- (d) Prohibited.

### **3.2 RISK FACTORS**

3.2.1 Risk shall be assessed based on:

- (a) country of residence;

- (b) source of funds;
- (c) occupation;
- (d) transaction patterns;
- (e) PEP (Politically Exposed Person) status.

### **3.3 RISK SCORING MODEL**

3.3.1 Each client shall be assigned a risk score based on:

- (a) geographic risk;
- (b) behavioral indicators;
- (c) financial profile consistency.

3.3.2 Risk scores shall determine:

- (a) onboarding requirements;
- (b) monitoring intensity;
- (c) approval authority.

## **4. CUSTOMER DUE DILIGENCE (CDD)**

### **4.1 IDENTIFICATION REQUIREMENTS**

4.1.1 The Company shall verify:

- (a) full legal name;
- (b) date of birth;
- (c) nationality;
- (d) residential address.

### **4.2 DOCUMENTATION**

4.2.1 Acceptable documents include:

- (a) passport / national ID (Proof of Identity – POI);
- (b) utility bill / bank statement (Proof of Address – POA).

### **4.3 VERIFICATION METHODS**

4.3.1 Verification shall be conducted through:

- (a) automated KYC systems (e.g. Sumsb);
- (b) manual review where required;
- (c) liveness checks where applicable.

#### **4.4 BENEFICIAL OWNERSHIP**

4.4.1 For corporate clients, the Company shall identify:

- (a) ultimate beneficial owners (UBOs);
- (b) ownership structure;
- (c) controlling persons.

### **5. ENHANCED DUE DILIGENCE (EDD)**

#### **5.1 HIGH-RISK CLIENTS**

5.1.1 EDD shall apply to:

- (a) high-risk jurisdictions;
- (b) PEPs;
- (c) complex ownership structures;
- (d) unusual transaction patterns.

#### **5.2 EDD REQUIREMENTS**

5.2.1 Additional measures include:

- (a) source of funds verification;
- (b) source of wealth assessment;
- (c) senior management approval;
- (d) enhanced monitoring.

#### **5.3 SOURCE OF FUNDS (SOF)**

5.3.1 Acceptable SOF evidence includes:

- (a) salary slips;

- (b) bank statements;
- (c) business income documentation;
- (d) inheritance or gift documentation.

## **6. ONGOING MONITORING**

### **6.1 TRANSACTION MONITORING**

6.1.1 The Company shall monitor:

- (a) deposit patterns;
- (b) withdrawal patterns;
- (c) trading behavior.

### **6.2 TRIGGERS FOR REVIEW**

6.2.1 Monitoring shall be triggered by:

- (a) large deposits;
- (b) sudden changes in activity;
- (c) inconsistent behavior.

### **6.3 PERIODIC REVIEW**

6.3.1 Client profiles shall be reviewed:

- (a) annually (high risk);
- (b) periodically (medium risk);
- (c) as required (low risk).

## **7. SUSPICIOUS ACTIVITY AND REPORTING**

### **7.1 SUSPICIOUS ACTIVITY**

7.1.1 Suspicious activity includes:

- (a) unexplained source of funds;
- (b) structuring transactions;
- (c) use of third-party accounts.

## **7.2 INTERNAL REPORTING**

7.2.1 Employees must report suspicious activity to the MLRO.

## **7.3 EXTERNAL REPORTING**

7.3.1 The MLRO shall file reports with relevant authorities where required.

## **8. SANCTIONS AND PROHIBITED CLIENTS**

### **8.1 SANCTIONS SCREENING**

8.1.1 The Company shall screen clients against:

- (a) international sanctions lists;
- (b) watchlists.

### **8.2 PROHIBITED CLIENTS**

8.2.1 The Company shall not onboard:

- (a) sanctioned individuals;
- (b) clients from prohibited jurisdictions.

## **9. RECORD KEEPING**

### **9.1 Retention**

9.1.1 Records shall be retained for a minimum of:

Seven (7) years

### **9.2 Scope**

9.2.1 Records include:

- (a) KYC documents;
- (b) transaction history;
- (c) monitoring logs.

## **10. TRAINING AND AWARENESS**

### **10.1 Staff Training**

10.1.1 Employees shall receive AML training on:

- (a) onboarding procedures;
- (b) suspicious activity detection;
- (c) reporting obligations.

## **11. ENFORCEMENT AND BREACH HANDLING**

### **11.1 NON-COMPLIANCE**

#### **11.1.1 Breaches may result in:**

- (a) disciplinary action;
- (b) termination;
- (c) reporting to authorities.