KYC/AML Policy for TAWT Token

Introduction

At Simplitaught, we are committed to maintaining the highest standards of integrity and compliance in all our operations. As the issuer of the TAWT token, we recognize the importance of implementing robust Know Your Customer (KYC) and Anti-Money Laundering (AML) policies to prevent illicit activities such as money laundering, terrorist financing, and fraud. This document outlines our comprehensive KYC/AML policies and procedures designed to ensure compliance with applicable laws and regulations.

1. Purpose

The primary objectives of our KYC/AML policies are to:

- Verify the identity of our customers and understand their financial activities.
- Assess and mitigate risks associated with money laundering and terrorist financing.
- Ensure compliance with legal and regulatory requirements.
- Protect Simplitaught and its stakeholders from reputational and legal risks.

2. Regulatory Framework

Our KYC/AML policies are developed by international standards and guidelines, including those set forth by the Financial Action Task Force (FATF). We also adhere to local regulations applicable in the jurisdictions where we operate. This includes compliance with the Bank Secrecy Act (BSA) in the United States and the 5th and 6th Anti-Money Laundering Directives (AMLD) in the European Union.

3. Scope

This policy applies to all customers engaging with Simplitaught's services involving the TAWT token, including but not limited to:

- Purchasing or selling TAWT tokens.
- Participating in token-based transactions within the Simplitaught platform.
- Engaging in any financial activities involving TAWT tokens.

4. Customer Identification Program (CIP)

To comply with KYC requirements, Simplitaught has established a Customer Identification Program that includes the following procedures:

4.1 Individual Customers

- **Information Collection**: We collect the following information from individual customers:
    - Full legal name.
    - Date of birth.
    - Residential address.
    - Government-issued identification number (e.g., passport or driver's license number).
- **Verification**: The collected information is verified using reliable, independent sources. This may include:
    - Valid government-issued identification documents.
    - Utility bills or bank statements as proof of address.
    - Biometric verification methods, where applicable.

4.2 Corporate Customers

- **Information Collection**: For corporate entities, we collect:
    - Legal entity name.
    - Registration number and jurisdiction.
      Principal place of business.
    - Details of directors and beneficial owners.
- **Verification**: Verification involves:
    - Reviewing incorporation documents.
    - Validating information against public and private databases.
    - Assessing the ownership and control structure to identify ultimate beneficial owners.

5. Customer Due Diligence (CDD)

Simplitaught conducts Customer Due Diligence to assess the risk profile of each customer. This process includes:

- **Standard Due Diligence**: Applied to all customers, involving identity verification and basic background checks.

- **Enhanced Due Diligence (EDD)**: For customers posing higher risks, such as politically exposed persons (PEPs) or those from high-risk jurisdictions, we implement additional measures, including:

    - In-depth analysis of the customer's source of funds and wealth.
    - Ongoing monitoring of transactions.
    - Senior management approval for establishing or continuing the business relationship.

6. Ongoing Monitoring

We continuously monitor customer transactions to detect and report suspicious activities. This includes:

- Real-time transaction monitoring to identify unusual patterns or behaviors.
- Regular reviews of customer information to ensure accuracy and relevance.
- Utilizing advanced analytics and blockchain analysis tools to trace and prevent illicit activities.

7. Record Keeping

Simplitaught maintains comprehensive records of all customer information, transaction data, and verification documents for a minimum period as required by applicable laws and regulations. These records are securely stored and protected against unauthorized access.

8. Reporting Obligations

In compliance with regulatory requirements, we promptly report any identified suspicious activities to the relevant authorities. This includes:

- Filing Suspicious Activity Reports (SARs) with appropriate regulatory bodies.
- Cooperating with law enforcement agencies during investigations.
- Complying with the "Travel Rule," which mandates the sharing of transaction details to prevent illicit fund transfers.

9. Training and Awareness

We provide regular training to our employees on KYC/AML policies, procedures, and the latest developments in financial crime prevention. This ensures that our team remains vigilant and capable of identifying and addressing potential risks effectively.

10. Data Protection and Privacy

We are committed to protecting the privacy and confidentiality of customer information. All data collected during the KYC/AML processes is handled by applicable data protection laws and our internal privacy policies.