AML CTF Policy

Last updated April 8, 2026

Anti-Money Laundering & Counter-Terrorism Financing (AML/CTF) Policy

AUDC Pty Ltd is committed to maintaining the highest standards of integrity, transparency, and compliance in all operations.
This policy outlines our approach to preventing, detecting, and responding to money laundering and terrorism financing risks.

1. Purpose and Scope

Purpose

The purpose of this AML/CTF Policy is to establish a strong framework to safeguard our platform and ecosystem from misuse.
It ensures compliance with applicable regulations, protects our stakeholders, and supports global financial security standards.

This policy is designed to:

- Ensure Compliance: Adhere to all applicable AML/CTF laws and regulations.
- Manage Risk: Identify, assess, and mitigate financial crime risks.
- Maintain Integrity: Prevent the use of our services for illicit purposes.
- Promote Awareness: Foster a strong internal culture of compliance.
- Support Transparency: Enable clear and accountable financial interactions.

Scope

This policy applies to all activities conducted by AUDC Pty Ltd across its global operations.

- All employees, directors, and management
- Business partners, affiliates, and service providers
- All customers and users of our services
- All products, platforms, and digital asset transactions
- All jurisdictions in which we operate

Compliance with this policy is mandatory. Failure to comply may result in disciplinary action or termination of services.

2. Regulatory Standards

AUDC Pty Ltd does not currently provide designated services under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) and is not required to be registered with AUSTRAC.

Notwithstanding this, we recognise that money laundering and terrorism financing are serious global risks.
We have implemented appropriate internal controls, procedures, and systems to manage these risks effectively.

3. Procedures and Guidelines

Money Laundering and Terrorism Financing

Money Laundering is the process of concealing the origin of funds derived from criminal activity. It generally occurs in three stages:

- Placement: Introducing illicit funds into the financial system
- Layering: Obscuring the origin through complex transactions
- Integration: Reintroducing funds as apparently legitimate assets

Terrorism Financing involves providing financial support to terrorist activities or organisations, including operational funding and network support.

Customer Information Requests

Where necessary, we may request additional information from customers to assess and manage risk.
Failure to provide requested information may result in restrictions or termination of services.

Customer Due Diligence (CDD)

We conduct appropriate verification of customers before providing services. This includes assessing legitimacy, regulatory compliance, and alignment with our risk framework.

Enhanced Due Diligence (EDD)

Additional checks may be conducted for higher-risk customers, including politically exposed persons (PEPs) or where suspicious activity is identified.

PEP and Sanctions Screening

We screen customers and associated parties against global sanctions lists and identify politically exposed persons to manage elevated risk.

Data Integrity

Customer information is verified using reliable, independent, and secure data sources, including government and regulatory databases.

Risk Assessment

We apply a risk-based approach considering customer type, transaction behaviour, geographic exposure, and service usage.

Transaction Monitoring

We monitor transactions to identify unusual or suspicious activity. This includes manual oversight and the planned implementation of automated monitoring technologies.

International Compliance

We align with international AML/CTF standards, including those set by the Financial Action Task Force (FATF), and support cross-border regulatory cooperation.

Address Blacklisting Approach

AUDD operates as a public, permissionless token and does not implement address blacklisting at a protocol level.
Instead, risk is managed through strict onboarding, monitoring, and oversight of authorised distributors.

Incident Reporting

Suspicious activities are escalated internally and assessed promptly. Appropriate action is taken in line with regulatory expectations and risk management procedures.

Privacy and Data Protection

We are committed to protecting customer privacy. Personal information is used solely for service provision, securely stored, and only accessible to authorised personnel.

We do not sell or share personal information with third parties except where required by law.