ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING (AML/CTF) POLICY

333D Limited ACN 118 159 881

Last updated: June 2026

1 PURPOSE

333D Limited ("**333D**" or the "**Company**") is committed to maintaining the highest standards of integrity, ethical conduct and regulatory compliance in all aspects of its operations.

This Anti-Money Laundering and Counter-Terrorism Financing (**AML/CTF**) Policy establishes the framework by which the Company seeks to identify, assess, manage and mitigate the risks of money laundering, terrorism financing, proliferation financing and other financial crime activities that may arise in connection with its business activities.

The Board recognises that effective AML/CTF controls are an important component of sound corporate governance and risk management and support the Company's commitment to protecting shareholders, stakeholders, employees, customers and business partners from financial crime. This policy has been developed having regard to the requirements of the Australian AML/CTF legislative framework and accepted international best practices

2 SCOPE

This Policy applies to:

- Directors;
- Officers;
- Employees;
- Contractors and consultants;
- Subsidiaries and controlled entities; and
- Any third party acting on behalf of the Company.

All persons covered by this Policy are required to comply with its provisions.

3 POLICY STATEMENT RESPONSIBILITIES

333D has a zero-tolerance approach to:

- Money laundering;
- Terrorism financing;
- Proliferation financing;
- Fraud;
- Corruption;
- Sanctions violations; and
- Any other form of financial crime.

The Company will not knowingly conduct business with any person, entity or organisation involved in unlawful activities or where there is a reasonable suspicion that funds or assets may be derived from criminal conduct.

The Company is committed to implementing appropriate systems, controls and procedures to identify and manage AML/CTF risks proportionate to the nature, scale and complexity of its operations.

4 OBJECTIVES

The objectives of this Policy are to:
- Prevent the Company from being used to facilitate money laundering or terrorism financing;
- Ensure compliance with applicable AML/CTF legislation and regulations;
- Protect the Company's reputation and shareholder value;
- Promote a culture of ethical business conduct;
- Support the identification and reporting of suspicious activities;
- Ensure appropriate due diligence is undertaken in relation to customers, investors, suppliers and business partners; and
- Establish clear responsibilities for AML/CTF compliance.

5 RISK-BASED APPROACH

33D adopts a risk-based approach to AML/CTF compliance.

The Company will periodically assess the AML/CTF risks associated with:

(a) Customers and Investors
Including:
- Shareholders;
- Investors;
- Joint venture participants;
- Strategic partners;
- Customers; and
- Other counterparties.

(b) Products and Services
Including:
- Capital raising activities;
- Equity investments;
- Acquisitions and divestments;
- Technology and healthcare services;
- Bitcoin treasury management activities;
- Digital asset transactions; and
- Other financial arrangements.

(c) Geographic Risk
Particular consideration will be given to transactions involving:
- High-risk jurisdictions;
- Sanctioned countries;
- Countries identified by the Financial Action Task Force (FATF); and
- Jurisdictions with weak AML/CTF controls.

(d) Transaction Risk
Including:
- Unusual transaction structures;
- Complex ownership arrangements;
- Transactions lacking apparent commercial rationale;
- Large or unusual payments; and
- Transactions involving virtual assets or digital currencies.

6 CUSTOMER AND COUNTERPARTY DUE DILIGENCE

The Company may undertake due diligence procedures appropriate to the risk profile of the relevant party. These procedures may include:

Standard Due Diligence
- Verification of identity;
- Verification of legal existence;
- Identification of beneficial owners;
- Verification of source of funds where appropriate; and
- Screening against sanctions and watchlists.

Enhanced Due Diligence
- Enhanced due diligence may be undertaken where higher risk circumstances exist, including:
- Politically exposed persons (PEPs);
- High-risk jurisdictions;
- Complex ownership structures;
- Significant investment transactions;
- Digital asset transactions; or
- Other circumstances identified by management.

Enhanced due diligence may include obtaining additional information regarding:
- Beneficial ownership;
- Source of wealth;
- Source of funds;
- Business activities; and
- Purpose of the relationship

7 BITCOIN AND DIGITAL ASSET ACTIVITIES

Given the Company's involvement in Bitcoin treasury management activities, the Company recognises the heightened AML/CTF risks associated with digital assets. Accordingly:

- Digital asset transactions shall only be undertaken through reputable and regulated service providers where practicable;
- Appropriate wallet and transaction monitoring controls shall be implemented;
- Counterparty verification shall be conducted for material transactions;
- Sanctions screening shall be undertaken where appropriate; and
- Transactions that present elevated AML/CTF risks may be declined or subjected to enhanced review.

8 MONITORING AND REPORTING

Management shall maintain procedures designed to identify and investigate unusual or suspicious activities. Indicators may include:
- Unexplained sources of funds;
- Transactions inconsistent with known business activities;
- Attempts to avoid identification procedures;
- Structuring of transactions to avoid reporting requirements;
- Requests involving sanctioned jurisdictions; or
- Unusual digital asset transaction patterns.

Where suspicious activity is identified, the matter must be escalated immediately to the Chief Executive Officer, Chief Financial Officer, Company Secretary, or another designated compliance officer.

9 SANCTIONS COMPLIANCE AND REPORTING

The Company will take reasonable steps to ensure compliance with applicable sanctions laws. The Company may:

- Screen counterparties against relevant sanctions lists;
- Restrict dealings with sanctioned persons or entities;
- Refuse transactions involving prohibited jurisdictions; and
- Seek external legal or compliance advice where required.

10 REVIEW

The Board will review this Policy periodically.

The Policy may be amended from time to time by resolution of the Board.