ANTI MONEY LAUNDERING, COUNTER TERRORIST FINANCING AND SANCTIONS POLICY

Last Updated: July 2026

Introduction

This Anti Money Laundering, Counter Terrorist Financing and Sanctions Policy is issued by

PERPETUAL LIQUIDITY LIMITED. Perpetual Liquidity Limited is an International Business Company registered in Saint Lucia under registration number 2024-00241, with its registered office located at Ground Floor, The Sotheby Building, Rodney Village, Rodney Bay, Gros Islet, Saint Lucia.

The purpose of this Policy is to describe the standards applied by the Company to prevent, detect and manage risks relating to money laundering, terrorist financing, proliferation financing, sanctions evasion, fraud, corruption and other financial crime.

This public policy summarises the Company's approach. Internal procedures, screening rules, risk scoring, escalation records and suspicious activity reports are confidential and are not disclosed to clients.

Core principles

- We do not open anonymous accounts or accounts in fictitious names.
- We only onboard clients whose identity, beneficial ownership and source of funds can be reasonably verified.
- We apply a risk based approach to client acceptance, due diligence and ongoing monitoring.
- We screen clients, beneficial owners, authorised persons and relevant counterparties against sanctions, PEP and adverse media sources.
- We reject, suspend or terminate relationships where the financial crime, sanctions or regulatory risk is unacceptable.
- We do not disclose suspicious activity reports or internal investigations to clients.

Governance and responsibility

The Company appoints a Money Laundering Reporting Officer or equivalent responsible person to oversee AML, CTF and sanctions compliance. The Company may also appoint deputies or external compliance support where appropriate.

The responsible person oversees client acceptance controls, sanctions screening, transaction monitoring, internal reporting, record keeping, employee awareness, policy review and suspicious activity escalation.

Client due diligence

Before establishing a relationship, and at appropriate times during the relationship, the Company may request documents, data and information to identify and verify the client, beneficial owners, controllers and authorised persons.

Individual clients

- Full legal name, date of birth, nationality, residential address and contact details.
- Valid identity document such as passport, national identity card or driving licence.
- Proof of residential address, where required.
- Information on employment, income, source of funds, source of wealth, trading experience and expected account activity.

Corporate clients

- Certificate of incorporation or equivalent formation document.
- Constitutional documents, register extracts or equivalent records.
- Registered office and principal place of business details.
- Ownership and control structure, including beneficial owners and controlling persons.
- Directors, authorised signatories, powers of attorney and account opening authorisations.
- Source of funds, source of wealth, nature of business and expected account activity.

Beneficial ownership

For legal entities, the Company seeks to identify natural persons who ultimately own or control the client. Where no natural person is identified through ownership or control, the Company may identify senior managing officials or other controlling persons in accordance with applicable law and internal procedures.

Risk assessment and enhanced due diligence

The Company assesses the financial crime risk of each client using factors such as jurisdiction, client type, ownership structure, product, payment method, source of funds, source of wealth, trading profile, expected account activity, sanctions exposure, PEP status and adverse media.

Enhanced due diligence may be applied to higher risk clients, complex structures, PEPs, high risk jurisdictions, unusual payment patterns, crypto related funds where accepted, high account turnover, third party involvement, adverse media or any matter that increases financial crime risk.

Enhanced due diligence may include senior management approval, additional source of funds or source of wealth evidence, independent verification, additional monitoring, lower limits, refusal of payment methods or termination of the relationship.

Sanctions and restricted jurisdictions

The Company screens against sanctions lists and may reject, block, freeze, suspend or terminate accounts where required by law or where risk is unacceptable.

The Company does not provide services to persons or entities that are subject to applicable sanctions or that are resident, incorporated, operating from, located in, or otherwise connected to jurisdictions where the Company determines that services are prohibited, restricted or outside its risk appetite.

The restricted jurisdictions list is reviewed periodically and may include jurisdictions subject to United Nations, United States, European Union, United Kingdom or other relevant sanctions, FATF calls for action, FATF increased monitoring, local prohibitions, licensing restrictions or internal risk decisions.

Deposits and withdrawals

The Company does not knowingly accept third party deposits or process third party withdrawals.

- Deposits and withdrawals must normally be made from and to payment methods held in the same name as the trading account holder.
- The Company may request additional evidence before processing any deposit or withdrawal.
- The Company may refuse, reverse, hold, return or delay a transaction where it has AML, CTF, sanctions, fraud, chargeback, legal, operational or risk concerns.
- Where a deposit was made by a particular method, the Company may require withdrawals to be returned through the same method before profits are withdrawn by another approved method.

Ongoing monitoring

The Company monitors account activity, payments, trading patterns and client information to assess whether activity is consistent with the client's known profile, expected activity and risk rating. The Company may request updated KYC documents and may restrict the account until the request is satisfied.

Suspicious activity and no tipping off

Employees and representatives must escalate suspicious activity internally without delay. Where required or appropriate, the Company may report suspicious activity to the relevant authority.

The Company will not notify a client that a suspicious activity report has been made or that an investigation is under way where doing so may breach law, regulation or internal policy.

Record keeping

The Company retains client identification records, account opening documents, transaction records, due diligence records, screening results, internal approvals, monitoring records and communications for at least seven years after the end of the relationship, or longer where required by law or justified by a legitimate business, legal or regulatory reason.

Training and review

Relevant employees and representatives receive AML, CTF and sanctions awareness appropriate to their role. This Policy is reviewed periodically and updated where required by legal, regulatory, sanctions, business or risk change