ANTI–MONEY LAUNDERING & COUNTER–TERRORIST FINANCING (AML/CTF) POLICY

VITTAVERSE LTD

0. Introduction and Status of this Policy

0.1 This Anti–Money Laundering & Counter–Terrorist Financing Policy (the “Policy”) explains how **Vittaverse Ltd**, incorporated in **St. Vincent & the Grenadines** (the “Company”, “we”, “us”, “our”), prevents and detects money laundering, terrorist financing, sanctions breaches, fraud, and other financial crime.

0.2 This Policy is **client-facing** and forms part of the contractual relationship between the Client and the Company where it is referenced and/or incorporated by reference into the Client agreement and/or other applicable terms.

0.3 This Policy is written to be **jurisdiction-neutral** and applies a **risk-based approach**. The Company will comply with **Applicable Regulations** and any lawful requests from competent authorities.

1. Definitions

For the purposes of this Policy:

1.1 **“Applicable Regulations”** means all laws, regulations, rules, sanctions programs, guidance, and binding obligations applicable to the Company and/or the Client, including AML/CTF obligations, as amended from time to time.

1.2 **“CDD” (Customer Due Diligence)** means identity verification and related checks performed on a Client.

1.3 **“EDD” (Enhanced Due Diligence)** means additional checks applied to higher-risk Clients.

1.4 **“PEP”** means a politically exposed person (including family members and close associates) as determined by screening and/or reliable information.

1.5 **“Beneficial Owner / UBO”** means the natural person(s) who ultimately owns or controls a legal-entity Client or on whose behalf an activity is conducted.

1.6 **“Report”** means a suspicious activity/transaction report or other required report made to a competent authority/financial intelligence unit (FIU) or another required reporting channel, as applicable.

2. Our AML/CTF Approach

2.1 The Company applies a risk-based approach to prevent and deter financial crime. This includes (without limitation):

a) identity verification (CDD/EDD);

b) screening for sanctions/PEP/adverse media indicators;
c) monitoring of deposits, withdrawals, and activity; and
d) taking actions required to comply with Applicable Regulations.

2.2 The Company has appointed an internal AML/Compliance function (including an AML Officer) responsible for oversight of AML/CTF controls.

3. Client Obligations

3.1 The Client must provide true, accurate, complete, and up-to-date information and documents requested for CDD/EDD and ongoing reviews.

3.2 The Client must promptly inform the Company of changes including (without limitation): name, address, residency, corporate ownership/control, directors, authorised signatories, source of funds/wealth, or any other material change relevant to CDD/EDD.

3.3 The Client must not attempt to:
a) deposit or withdraw using third-party payment methods;
b) conceal the origin/ownership of funds;
c) circumvent controls, monitoring, or verification; or
d) use the Company's services for unlawful purposes.

4. Customer Due Diligence (CDD)

4.1 The Company may conduct CDD:
a) before opening an account;
b) before allowing deposits/withdrawals;
c) before permitting trading or certain products; and/or
d) at any time thereafter (periodic review or trigger-based review).

4.2 For individual Clients, CDD may include verifying identity, address, and payment-method ownership, and may include source of funds/wealth information.

4.3 The Company may refuse to open an account, restrict services, or suspend withdrawals until CDD is completed to the Company's satisfaction.

5. Legal Entity Clients (Corporate CDD and Beneficial Ownership)

5.1 The Company accepts legal entity Clients and applies corporate due diligence, which may include:
a) proof of incorporation/registration and company details;
b) registered address and principal place of business;
c) directors and authorised signatories verification;
d) verification of Beneficial Owners/UBOs;
e) evidence of authority for persons acting on behalf of the entity; and
f) business activity, expected account use, and source of funds/wealth (as applicable).

5.2 If the Company cannot reasonably identify or verify the Beneficial Owners/UBOs or the control structure, the Company may refuse onboarding, restrict services, or terminate the relationship.

6. Enhanced Due Diligence (EDD)

6.1 The Company may apply EDD where risk is higher, including (without limitation):
a) PEPs or PEP-linked parties;
b) high-risk jurisdictions;
c) unusual funding/withdrawal behaviour;
d) higher-risk payment methods or crypto-related activity;
e) adverse media indicators; or
f) suspicious activity signals.

6.2 EDD may require additional documents, explanations, and/or limits or restrictions on account activity.

7. Sanctions, PEP, and Screening

7.1 The Company may screen Clients, legal entity controllers, Beneficial Owners/UBOs, directors, and authorised persons against sanctions lists, PEP databases, and adverse media sources.

7.2 If screening indicates elevated risk, potential sanctions exposure, or suspicious activity, the Company may request additional information, restrict or freeze the account, refuse transactions, file a Report where required, and/or terminate the relationship.

8. Monitoring and Reviews

8.1 The Company may monitor account activity, deposits, withdrawals, and related behaviours to identify unusual or suspicious patterns.

8.2 The Company may request explanations and documentation regarding activity, including source of funds/wealth and the economic purpose of transactions.

9. Deposits, Withdrawals, and Payment Rules

9.1 Third-Party Payments Strictly Prohibited

9.1.1 All deposits and payments must be made only from accounts or payment instruments belonging to the Client. Third-party payments are strictly prohibited.

9.1.2 The Company may reject, reverse, return, or freeze funds associated with third-party payments and may require proof of payment-method ownership at any time.

9.2 Withdrawal Controls (Operational Rights)

9.2.1 To comply with Applicable Regulations and manage AML/CTF risk, the Company may, at its sole discretion:
a) decline a withdrawal request or withdrawal method;
b) request additional documentation prior to processing;
c) delay processing pending verification/review;
d) reverse a withdrawal request and return the amount to the trading account/wallet where appropriate; and/or
e) require withdrawals to be made only to verified instruments belonging to the Client.

9.2.2 Where a withdrawal is declined, reversed, returned, or re-routed, the Client bears any charges imposed by banks/payment providers and/or network fees.

9.3 Proportional Withdrawals (Return-to-Source Model)

9.3.1 Withdrawals are processed using a proportional “return-to-source” logic:
a) First, withdrawals are processed back to the same funding method(s) up to the same amount deposited through each method (or as close as operationally feasible), based on the Company’s records;
b) Then, any remaining amount may be withdrawn via other verified withdrawal methods belonging to the Client, subject to verification, risk checks, and Company approval.

9.3.2 The Company may deviate from this flow where required by Applicable Regulations, payment-provider rules, operational constraints, or risk controls.

9.4 Cryptoasset Deposits and Withdrawals

9.4.1 Where cryptoasset funding is offered, the Company may:
a) require transaction hashes and supporting evidence;
b) apply blockchain risk checks;
c) restrict withdrawals to previously used and/or verified wallet addresses; and
d) refuse, delay, or freeze transactions linked to high-risk sources or suspicious indicators.

9.5 Unacceptable Payments and Remedies

9.5.1 Payments may be deemed unacceptable where they involve (without limitation) third-party funding, fraud/chargeback risk, sanctions exposure, inconsistent ownership evidence, or suspicious indicators.

9.5.2 In such cases, the Company may reverse/return funds to the original source where feasible, restrict or freeze the account, request additional verification, file a Report where required, and/or terminate the relationship.

10. Company Rights to Restrict, Freeze, Refuse, Reverse, and Close

10.1 The Company may, at its sole discretion and without prior notice where necessary, take actions to comply with Applicable Regulations or manage AML/CTF risk, including:
a) freezing or restricting accounts/wallets;
b) suspending deposits/withdrawals;
c) refusing, delaying, reversing, or cancelling transactions;
d) requesting additional information or documentation; and/or
e) closing accounts and terminating the relationship.

10.2 The Company is not required to disclose details of internal assessments or thresholds used to detect suspicious activity where such disclosure could prejudice risk controls or where restricted by Applicable Regulations.

11. Reporting and No Tipping Off

11.1 Where required or appropriate, the Company will file a Report with the relevant competent authority/FIU and will cooperate with lawful requests from authorities.

11.2 No Tipping Off**:** The Company, its staff, and its agents will not inform the Client (or any other person) that a Report has been filed (or may be filed) or that an investigation is underway, where such disclosure is prohibited or could prejudice an investigation.

12. Record Keeping

12.1 The Company retains AML/CTF-related records (including CDD/EDD documents and transaction records) for at least five (5) years, or longer if required by Applicable Regulations or an ongoing investigation.

13. Restricted Countries

13.1 As part of its risk controls and sanctions compliance, the Company does not accept Clients from and/or does not provide services to certain jurisdictions.

13.2 As of the date of this Policy, restricted jurisdictions include:

- **United States of America (USA)**
- **Canada**
- **United Kingdom**
- **Japan**
- **North Korea**

13.3 This list may be updated from time to time based on sanctions, risk appetite, and Applicable Regulations.

14. Policy Updates

14.1 The Company may update this Policy from time to time. Updated versions will be made available on the Company Website and/or upon request. Continued use of the Company's services after an update constitutes acceptance of the updated Policy to the extent permitted by Applicable Regulations.

15. Governing Terms

15.1 This Policy should be read together with the Client agreement and other applicable terms. In case of inconsistency, the Company will apply the documents in the order of precedence stated in the Client agreement (or, if not stated, in a manner consistent with Applicable Regulations and the purpose of AML/CTF controls).

Governing Language

In the event of any discrepancy between translations, the **English version shall prevail**.

Company Information

Vittaverse Global Markets Ltd
Website: https://vittaverse.com
Email: compliance@vittaverse.com

Document Version: VT-AML-001
Last Updated: 2026