Stockity Anti-Money Laundering Policy

(hereinafter referred to as the "Policy")

Section 1: Interpretative Provisions

For the purposes of this Policy, the following definitions shall apply consistently, whether referenced in singular or plural form:

1.1 ***Account*** means any account, facility, or service maintained by a Client with the Company through the Company's Platform.

1.2 ***Company*** / **We / Us / Our**, means Verte Securities Limited, a company incorporated under the laws of the Republic of Vanuatu, bearing registration number: 700726, with its registered office located at: Level 1, iCount House, Kumul Highway, Port Vila, Vanuatu.

1.3 ***Client*** means any natural person or legal entity that establishes, maintains, or seeks to establish a business relationship with the Company.

1.4 ***Funds*** mean money and its equivalents applicable to the authorized activities on the Platform.

1.5 ***Platform*** refers to the Company's proprietary trading and Client service systems, including electronic platforms, applications, and related technological infrastructure.

1.6 ***Reporting Entity*** means Verte Securities Limited in its capacity as an entity subject to the obligations under the Anti-Money Laundering and Counter-Terrorism Financing Act No. 13 of 2014 and its amendments.

1.7 ***Suspicious Transactions*** means any transaction on or off the Platform that the Company reasonably suspects may breach laws or regulations, be linked to terrorist financing or activities (individuals, organizations, or assets), display complexity, unusual structure, or atypical patterns, lack an obvious lawful or economic rationale, or fall outside normal transactional behavior.

1.8 ***Suspicious Activities*** means any transaction or series of transactions where there is reason to believe the individual is engaged in money laundering or financing of terrorist activities.

1.9 ***Vanuatu Financial Intelligence Unit (VFIU)*** means the financial intelligence unit established within the Office of the Attorney General pursuant to the Anti-Money Laundering and Counter-Terrorism Financing (Amendment) Act No. 16 of 2024.

Section 2: Risk-Based Approach Framework

2.1 Risk Assessment Methodology

The Company implements a comprehensive risk-based approach to AML/CFT compliance, consistent with the requirements of Vanuatu legislation and international best practices including FATF Recommendations and FIU Guidance Notes (VFIU). This approach involves the systematic identification, assessment, and mitigation of money laundering and terrorist financing risks associated with: Client categories and geographical locations; Products and services offered; Transaction patterns and delivery channels; Jurisdictional risk factors.

2.2 Enhanced Due Diligence Triggers: enhanced due diligence measures are implemented when Clients or transactions present heightened risk factors, including but not limited to: Politically Exposed Persons (PEPs) and their family members or close associates; Clients from high-risk and sanctioned jurisdictions identified by international bodies; Complex corporate

structures with unclear beneficial ownership; Unusual transaction patterns inconsistent with Client profiles; Client Due Diligence Framework.

Section 3: Client Identification and Verification

Identity Verification Documents:	Additional Documentation (KYC/AML Compliance)
A clear photograph of the Client's passport data page or national identity card; Images of the Client's bank cards or screenshots of their electronic wallets; A recent selfie of the Client holding the above document(s) in hand.	A utility bill issued within the last 3 (three) months; A bank confirmation letter dated not more than 3 (three) months ago; A bank statement (letter form) no older than 3 (three) months; Evidence of the source of funds or wealth (e.g., payslips, property sale contracts, loan agreements, inheritance documents); A secondary ID (for example, a valid driving license); Notarized copies of any of the above.

3.1 The Client sends all requested documents as JPG, JPEG or PDF attachments via email to our Compliance Department at verification@stockity.com. We cannot accept RAR/ZIP archives or DOC/DOCX files. All materials must be delivered within fourteen (14) calendar days of our request. Upon receipt of a complete document set, verification is normally completed within twenty (20) minutes. In certain circumstances, this timeframe may be extended up to seven (7) calendar days.

3.2 If further confirmation is needed, We will arrange a live video verification via Zoom or a similar platform.

3.3 To ensure uninterrupted and compliant KYC/AML procedures, We may engage vetted third-party verification partners who adhere to applicable legal and regulatory standards. For details, refer to Our Privacy Policy at https://stockity.com/information/privacy.

3.4 Detailed Document Requirements

- *General ID Documents*: all sides of the passport or ID must be fully visible in the image, with no cropping, glare, or obstructions. The document's text must be sharp and legible; the holder's signature may be obscured. The Client must be at least the legal age of majority, and the ID must be valid. Watermarks are acceptable. Images will be checked for signs of editing or manipulation.

- *Validity Checks*: if authenticity is in question, we may use AML database services (including global watchlists: OFAC, UN, EU, and law enforcement or regulatory registries) to verify document legitimacy.

- *Bank Card Criteria*: photograph the card so all corners are visible, without glare. The following must be legible: cardholder's full name; first six and last four digits of the card number; expiry date.

*If the card does not bear the Client's name, we may request a screenshot from the online banking portal showing the full name or an official bank statement (with cardholder name, partial card number, bank stamp and signature).

- *Electronic Wallets*: provide 2 (two) screenshots:

    a. A deposit transaction to Verte Securities Limited, showing date, time, amount and wallet ID.

    b. The wallet's personal information page, displaying first and last name (and date of birth, if available).

Ensure both images clearly come from the same e-wallet interface.

- *Selfies with Documents*: the Client's face and the entire ID must be clearly visible and match the document photo (accounting for age). The document held in the selfie must be identical to the one in the standalone scan.

- *Translations*: non-English documents require a notarized English translation and the original's clear image. Our third-party verifiers will also accept translated materials in compliance with data-protection laws.

3.5 The measures indicated herein are designed not only to comply with Our KYC/AML Policy but also to safeguard the security of Client assets.

3.6 Deposits of Funds: the name of the depositor (Client) of Funds should fully comply with the name specified in the registered Account (if the payment system provides the name of the depositor (Client) of Funds) for successful completion of the procedure for crediting Funds. Payments from third parties are prohibited. The Company has the right to demand strict adherence to the accepted procedure for depositing and withdrawing Funds.

WE HEREBY DECLARE THAT, IN ORDER TO COMPLY WITH THIS AML POLICY, TRANSFERS OF FUNDS BY THE CLIENTS ARE PERMITTED SOLELY FOR THE PURPOSE OF CARRYING OUT TRADING OPERATIONS ON THE PLATFORM. IF THE COMPANY REASONABLY BELIEVES THAT TRANSFERS OF FUNDS ARE BEING USED BY THE CLIENT IN VIOLATION OF LAWS AND/OR OUR AML POLICY, AND/OR FOR THE PURPOSES OTHER THAN THE COMPANY'S SERVICES OFFERED, THE COMPANY RESERVES THE RIGHT TO BLOCK THE CLIENT'S ACCOUNT TO PREVENT SUCH A VIOLATION.

Section 4: Measures Against Suspicious Transactions and Activities

4.1 If any indicators of fraud emerge during the execution of financial transactions—after Funds have been credited to the Client's Account — We may cancel those transactions and the Client's Account.

4.2 Should it become evident that the Client intends to use their Account solely to exchange funds between payment systems, We reserve the right to refuse any withdrawal requests.

4.3 If We suspect the Client of fraudulent or deceitful conduct, we may block the Client's Account immediately, without prior notice or the opportunity to withdraw Funds.

ALL SUCH RISK-MITIGATION ACTIONS WILL BE REPORTED, AS PROMPTLY AS PRACTICABLE, TO THE APPROPRIATE GOVERNMENTAL AUTHORITY WHENEVER OUR AML/CFT COMPLIANCE TEAM KNOWS, SUSPECTS, OR HAS REASONABLE GROUNDS TO BELIEVE THAT THE CLIENT IS INVOLVED IN MONEY LAUNDERING OR TERRORIST FINANCING, OR THAT A TRANSACTION IS INTENDED FOR THOSE PURPOSES UNDER APPLICABLE ANTI-MONEY LAUNDERING REGULATIONS.

Section 5: Document Submission and Processing

5.1. Clients must provide verification documents in digital format through secure channels. The Company accepts documents in the following formats: JPEG, PNG, PDF, and TIFF. Documents must be clear, legible, and demonstrate the authenticity features of the original documents. All non-English documents must be accompanied by certified translations prepared by qualified translators. The translation must be notarized and submitted alongside high-resolution images of the original documents.

5.2 The Company maintains strict security protocols for document handling: encrypted transmission channels for all document submissions, secure storage systems with access controls and audit trails, regular security assessments and penetration testing of document management systems.

5.3 The Company employs multiple verification methodologies to ensure the authenticity of Client information: Enhanced Digital Verification (video verification sessions conducted via secure platforms / real-time document authentication using optical character recognition / biometric verification where technologically feasible) or Manual Review Processes (expert review of complex cases by qualified compliance officers / cross-referencing with multiple data sources and databases / secondary verification for high-risk Client categories / transaction monitoring and reporting).

Section 6: Ongoing Due Diligence Obligations

6.1. Pursuant to the ongoing due diligence obligations under Vanuatu law, the Company maintains continuous monitoring of all Client relationships and transactions. This monitoring ensures that: (i) transactions remain consistent with the Company's knowledge of the Client; (ii) business activities align with stated purposes and risk profiles; (iii) unusual patterns or suspicious activities are promptly identified; (iv) Client information remains current and accurate.

6.2 The Company implements reporting mechanisms consistent with Vanuatu's transaction reporting requirements:

a. Suspicious Transaction Reports (STRs): all transactions suspected of involving proceeds of crime or terrorist financing must be reported to the VFIU within two working days of identification.

b. Large Transaction Reports: transactions exceeding prescribed thresholds are subject to enhanced monitoring and potential reporting requirements as established by VFIU guidelines.

c. Cross-Border Transaction Monitoring: particular attention is paid to cross-border transactions, especially those involving high-risk jurisdictions or complex routing arrangements.

Section 7: Sanctions Screening and Compliance

7.1 We maintain comprehensive sanctions screening procedures utilizing:

- United Nations Security Council sanctions list;
- OFAC sanctions list;
- EU sanctions list and maps;
- Vanuatu domestic sanctions measures;
- International sanctions regimes including those maintained by major financial centers;
- Regional sanctions frameworks applicable to Vanuatu's jurisdiction.

7.2 Our advanced screening technology incorporates: real-time screening against consolidated sanctions databases; name-matching algorithms with fuzzy logic capabilities; periodic re-screening of existing Client bases; transaction screening for sanctions-related indicators.

Section 8: Record Keeping and Data Retention

8.1 In compliance with Vanuatu's record-keeping obligations, We maintain all Client due diligence records, transaction records, and compliance documentation for a minimum period of six years following the cessation of the business relationship or completion of the transaction.

8.2 We implement robust data protection measures ensuring:

i. Confidentiality of Client information in accordance with privacy laws;

ii. Secure data storage with appropriate access controls;

iii. Regular backup procedures and disaster recovery protocols;

iv. Compliance with applicable data protection regulations.

Section 9: Compliance Officer Responsibilities

9.1 In accordance with the requirements of the Anti-Money Laundering and Counter-Terrorism Financing Act, the Company has appointed a qualified AML/CFT Compliance Officer responsible for:

1) Overseeing the implementation and effectiveness of the AML/CFT program;
2) Ensuring compliance with all applicable laws and regulations;
3) Maintaining relationships with regulatory authorities and law enforcement;
4) Coordinating suspicious transaction reporting and regulatory communications.

Section 10: Cross-Border Transaction Management

We implement enhanced due diligence for international wire transfers, consistent with FATF Recommendation 16 and Vanuatu's wire transfer obligations, including:	We maintain correspondent banking relationships, enhanced due diligence includes:
Complete originator and beneficiary information verification; Enhanced screening for transactions involving high-risk jurisdictions; Documentation of the purpose and nature of cross-border transfers; Compliance with travel rule requirements for virtual asset transactions where applicable.	Assessment of correspondent institutions' AML/CFT programs; Clear definition of roles and responsibilities; Regular monitoring of correspondent banking activities; Termination procedures for unsatisfactory relationships.

Section 11: Enterprise Risk Management Integration

AML/CFT risks are integrated into the Company's broader enterprise risk management framework through:	Business Line Risk Management: each business line maintains specific risk management procedures including:
Regular risk assessments and updates to risk profiles; Integration with operational risk management processes; Coordination with compliance and legal risk functions; Reporting to senior management and board committees.	Product-specific risk assessments and mitigation measures; Client onboarding procedures tailored to risk levels; Transaction monitoring parameters appropriate to business activities; Regular review and update of risk management procedures.

Section 12: Asia-Pacific Engagement

12.1 As a member of the Asia/Pacific Group on Money Laundering (APG), Vanuatu participates in regional cooperation initiatives. We support these efforts through: compliance with regional best practices and standards; participation in information sharing where appropriate; support for regional capacity building initiatives; alignment with regional risk assessments and priorities.

12.2 We ensure compliance with international standards including: Financial Action Task Force (FATF) recommendations and guidance; Basel Committee on Banking Supervision guidelines where applicable; International Organization of Securities Commissions (IOSCO) principles; United Nations conventions and protocols on money laundering and terrorism financing.

THE POLICY BASED ON THE AUTHORITY OF VANUATU'S COMPREHENSIVE ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING LEGISLATIVE FRAMEWORK, WHICH INCLUDES:

Anti-Money Laundering and Counter-Terrorism Financing Act No. 13 of 2014

Anti-Money Laundering and Counter-Terrorism Financing (Amendment) Act No. 16 of 2024

Counter Terrorism and Transnational Organized Crime Act [CAP 313]

Financial Institutions Act No. 2 of 1999

Companies Act No. 25 of 2012

Proceeds of Crime Act [CAP 284]

If you have any additional questions, please contact Us via email: verification@stockity.com