ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM POLICY

Effective Date:November 2025

Version: 1.0

ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM POLICY

For: VG MARKETS (Pty) Ltd
FSP Number: 54461
Effective Date: November 2025
Version: 1.0
Policy Owner: Chief Compliance Officer / MLRO

1. POLICY STATUS AND STATEMENT OF PRINCIPLES

1.1. VG MARKETS (Pty) Ltd ("the Company"), a licensed Financial Services Provider (FSP No. 54461) regulated by the Financial Sector Conduct Authority ("FSCA"), is categorised as an Accountable Institution under the Financial Intelligence Centre Act, No. 38 of 2001 ("FICA"), as amended. The Company is irrevocably committed to the highest standards of compliance with all applicable laws and regulations concerning Anti-Money Laundering ("AML"), Combating the Financing of Terrorism ("CFT"), and Countering Proliferation Financing ("CPF"). This Policy sets out the principles and governance framework adopted by the Company.

1.2. The objective of this Policy is to prevent the Company from being used for money laundering, terrorist financing, or proliferation financing.

1.3. This Policy is an internal governance document and does not form part of any client agreement or contract, is not intended to be contractually binding, and creates no third-party rights or obligations for the Company beyond those expressly mandated by FICA or other applicable law. The Company reserves all rights at law and in equity. It is provided for informational purposes only.

2. GOVERNANCE AND OVERSIGHT

2.1. The Board of Directors retains ultimate responsibility for AML/CFT compliance. The Board delegates day-to-day authority to the appointed **Money Laundering Compliance Officer ("MLRO")**, who operates with independence, sufficient seniority, and resources.

2.2. The MLRO shall, among other things, be responsible for:

2.2.1. Implementing this Policy,

2.2.2. Monitoring and reporting of all suspicious transactions and sharing of information as required under the Act and related regulations,

2.2.3. Overseeing and ensuring overall compliance with regulatory guidelines on AML & CFT issues from time to time,

2.2.4. Developing appropriate compliance management arrangements across the full range of AML & CFT areas (e.g. CDD, record keeping, etc.),

2.2.5. Maintaining close liaison with the Financial Intelligence Centre ("FIC"), FSCA, other designated institutions and any other institutions, which are involved in the fight against money laundering and combating financing of terrorism,

2.2.6. Authorising Suspicious Transaction Reports ("STRs"), overseeing the Risk Management and Compliance Programme ("RMCP"), and ensuring staff training.

2.3. The Company shall ensure that the MLRO is able to act independently and report directly to the governing board.

2.4. The Company shall ensure that the MLRO and other appropriate staff members have timeless access to client identification data and other CDD information, transaction records and other relevant information.

2.5. The Company shall provide the MLRO with the necessary access to systems and records to enable him/her to investigate and validate internal suspicious reports which would have been reported to him/her.

3. RISK MANAGEMENT AND COMPLIANCE PROGRAMME (RMCP)

3.1. The Company maintains a dynamic, risk-based RMCP as per Section 42 of FICA. The RMCP identifies, assesses, and mitigates ML/TF/PF risks associated with its customers, countries, products, services, and delivery channels.

3.2. **Risk-Based Approach (RBA):** The Company's application of Customer Due Diligence ("CDD"), Enhanced Due Diligence ("EDD"), and ongoing monitoring is proportionate to the risks identified. The Company's determination of a customer's risk rating (Low, Medium, High, Prohibited) and the corresponding controls applied is final and conclusive, based on its internal methodology.

3.3. The risk assessment shall be based on:

3.3.1. The nature, scale and complexity of the client ’s operations, including geographical diversity;

3.3.2. The initial and on-going due diligence or monitoring conducted on the client;

3.3.3. Any previous relationships with the applicant or other parties to the application;

3.3.4. Time scale, especially in relation to early encashment (whether for the current application or previous transactions);
3.3.5. The nature of the client, product, and activity profile;
3.3.6. The nature of the business relationship (i.e. occasional vs. on-going relationship);
3.3.7. The volume, frequency and size of transactions; and
3.3.8. The extent to which the Company is dealing directly with clients or is dealing through intermediaries, third parties or in a non-face-to-face setting.

3.4. The following measures and controls to mitigate the potential money laundering and terrorism financing risks for situations that are considered to be of higher risk as a result of the risk assessment shall be considered:
3.4.1. Increased levels of KYC or enhanced due diligence, such as proactive contact with the client to determine the reason for the transactions and the source of funds;
3.4.2. Increased levels of controls and frequency of reviews of client relationships;
3.4.3. Increased transaction monitoring of higher-risk products, services and channels; and
3.4.4. Enhanced systematic controls and data integrity at the points of payment, particularly at higher risk agent location.

4. CUSTOMER DUE DILIGENCE (CDD) & KNOW YOUR CLIENT (KYC)

4.1. The Company is mandated to know/understand its clients and their financial dealings better, which in turn helps in identifying suspicious transactions and managing of risk.
4.2. An on-going CDD should be performed. CDD includes identifying, verifying and monitoring all aspects of the client's identity, residential address, any temporary address, and includes information on the source of funds and source of wealth. It also includes information relating to any beneficial owner who has an interest in the securities, or controller who exercises influence over the investment.
4.3. The Company shall implement a risk-based CDD.
4.4. The Company shall implement the following procedures regarding "Know Your Client":
4.4.1. Verify and document the true identity of the clients that establish a relation, open accounts or conduct significant transactions, according to FICA and internal business procedures.
4.4.2. Obtain and document any additional information on the client based on the risk per activity.

4.4.3. Make sure that business transactions are carried out with companies or persons whose identities cannot be confirmed, failing to provide the required information or that provide false information or containing significant inconsistencies that cannot be satisfied after a further investigation.

4.4.4. In the case of natural persons, the respective official identification document or any other reliable document should be requested to verify the identity thereto.

4.4.5. In the case of legal persons, the company's incorporation document and any information related to its main activity, address, key controllers, among others must be obtained.

Account should only be named after the real name of the client, unless otherwise allowed by the law.

4.5. The Company reserves the absolute right, at any time before, during, or after the establishment of a relationship, to request any documentation or information it deems necessary to verify a client's identity, source of funds, wealth, or the purpose of a transaction. Failure to provide such information promptly and satisfactorily is grounds for immediate refusal or termination of services.

4.6. The Company will not accept the following clients:

4.6.1. Persons or institutions of questionable honesty, especially if they are related with drug traffic, money laundering, terrorism or any organized crime.

4.6.2. Persons or institutions with business which are difficult to know the real source of their money.

4.6.3. Accounts with false names, anonymous or pseudonym instead of the real name of the client.

4.6.4. Nominee accounts, where the details of the beneficial owners will not be provided on request or difficult to be ascertained.

4.7. All documents required for the purposes of identifying and verifying a client should not be **more than 3 months old**, and any certified documents should be certified by a recognised certifier.

4.8. Certifiers are required to sign under seal, state is/her name in block capitals, telephone number, profession, name and address of business or official stamp, and date on which the document is being certified. The certifier should not be closely related to the person whose identity is being certified (e.g. immediate family member, spouse, etc.).

4.9. The Company shall, where necessary, carry out independent verifications to verify any document provided by the client for the purposes of identifying and verifying clients.

4.10. The Company may outsource the services of any independent party to act on its behalf, for such purposes.

4.11. Whenever the Company engage with an intermediary or third party to introduce business, it shall:

4.11.1. Immediately obtain the account opening information.

4.11.2. Ensure the intermediary or third party provides the key account opening documents upon request as soon as possible (should the Company allow the intermediary or third party to keep the documents on its behalf, the Company understands it will assume all the risks attendant to the decision and arrangement); and

4.11.3. Satisfy itself that the intermediary or third party is regulated and supervised for and has measures in place to comply with FICA.

5. ENHANCED DUE DILIGENCE (EDD)

5.1. EDD is applied to high-risk customers, including Politically Exposed Persons (PEPs), Prominent influential Persons (PIPs), and high-risk jurisdictions.

5.2. The Company shall from time to time adopt and utilise, as a minimum, the FATF high risk countries list, as the basis for classifying risk countries.

6. POLITICALLY EXPOSED PERSONS (PEPs) AND PROMINENT INFLUENTIAL PERSONS (PIPs)

6.1. PEPs are the persons who perform or have performed public positions in the Republic of South Africa or abroad, including the high Officers of the Executive, Legislature and Judiciary, the Public Ministry, the high Military Commands, Senior Executives and State Companies Directors, the country main cities Mayors and main political parties' representatives.

6.2. PIPs are the extended term from PEPs that includes other persons of significant local influences.

6.3. The Company identifies and screens for: - Foreign PEPs; - Domestic PEPs; - PIPs and their immediate family members and close associates.

6.4. The following control shall be taken about PIPs clients:

6.4.1. If during commercial relationship, a client is classified as PEP/PIP; then the client must be registered as such in a database, and approval for keeping the said relationship must be provided by the Chief Compliance Officer or by the official on whom this responsibility has been delegated.

6.4.2. Gather sufficient information on any person/client of this category intending to undertake a transaction and check all the information available on the person in the public domain.

6.4.3. Apply enhanced client due diligence when verifying the identity of the PEP/PIP and seek information about the source/s of wealth and source/s of funds before accepting the PEP/PIP as a client.

6.4.4. The decision to undertake a transaction with a PEP/PIP shall be taken by the Chief Compliance Officer or by the official on whom this responsibility has been delegated. The PEP transactions should be subject to enhanced monitoring on an on-going basis.

7. SANCTIONS AND TARGETED FINANCIAL SANCTIONS(TFS)

7.1. The Company screens customers and transactions against: - United Nations Security Council sanctions list; - Applicable domestic and international sanctions lists.

7.2. In terms of **section 26A of FICA**, the Company shall immediately freeze property linked to sanctioned persons without prior notice and report such action to the FIC.

8. ONGOING MONITORING AND SUSPICIOUS TRANSACTIONS

8.1. The Company conducts ongoing monitoring of all relationships to ensure transactions are consistent with the customer's profile and risk rating.

8.2. The ongoing monitoring shall include:

8.2.1. Transaction pattern analysis.

8.2.2. Periodic CDD refresh.

8.2.3. Event-driven review.

8.3. **Suspicious Transaction Reporting (STR):** Any employee who suspects a transaction involves proceeds of unlawful activity or terrorism financing must immediately report internally to the MLRO. The MLRO will evaluate and, where there are reasonable grounds for suspicion, file an STR with the FIC via the goAML platform.

8.4. **Prohibition on Tipping-Off:** It is a criminal offense to disclose to a customer or any third party that an STR has been or will be filed, or that an investigation is underway. All staff are bound by this prohibition.

8.5. **Consequences of STR Filing:** Upon filing an STR or during an investigation, the Company reserves the right, in its sole discretion and without prior notice, to: (i) block or suspend the client's account(s); (ii) refuse to execute any instruction; (iii) delay or withhold any payment or withdrawal; and (iv) terminate the business relationship. The Company shall not be liable for any loss, damage, or expense incurred by the client as a result of such actions taken in good faith to comply with the law.

9. TRANSACTION AND FUNDS CONTROLS

9.1. The Company does not accept physical delivery in cash.

9.2. **Deposits:** The Company does not accept third-party deposits. Funds must originate from an account in the exact name of the registered client. The Company may reject any deposit if the source cannot be verified to its satisfaction.

9.3. **Withdrawals:** Withdrawals shall be made only to the account and via the method from which the funds originated (the "Same Origin Method" principle). The Company may, at its discretion, require additional verification for any withdrawal, decline a specific payment method, or impose a cooling-off period.

9.4. Where applicable thresholds are triggered, the Company shall submit:

9.4.1. **Cash Threshold Reports (CTRs) –** refers to the report that must be submitted to the FIC where a transaction is concluded with a client, and an amount of cash in excess of the prescribed amount, that is, R24, 999 is paid or received by the company in terms of that transaction. The cash threshold also includes a series of transactions or an aggregate of smaller amounts which when combined equal the amount of R24, 999. If it appears to the company that the transactions involving those smaller amounts are linked, these transactions must be considered as fractions of one transaction.

9.4.2. **Other statutory reports** that required under FICA.

9.5. **Right to Retain Funds:** Where suspicious activity is identified, the Company reserves the right to retain and segregate any funds suspected of being proceeds of crime or related to ML/TF/PF, pending investigation or directive from competent authorities. The Company may charge reasonable administrative fees for investigations necessitated by client behaviour.

10. RECORD KEEPING, DATA SHARING AND CONFIDENTIALITY

10.1. Records, including CDD documents, transaction data, and STR files, will be maintained for **at least five (5) years** following the termination of the relationship, as required by FICA.

10.2. The Company shall take appropriate steps to evolve and maintain a system that allows data to be retrieved easily and quickly whenever required, or when requested by competent authorities.

10.3. In the event that the Company outsource the record keeping responsibility to a third party, the Company acknowledges that it shall assume full responsibility and risk associated with the arrangement and shall ensure that the third party provides the requested documents within seven days.

10.4. **Client Consent to Disclosure:** By engaging with the Company, the client expressly acknowledges and consents that the Company may disclose any client information, personal data, or transaction details without prior

notice to:

* (a) The FIC, FSCA, or any other South African regulatory or law enforcement body;
* (b) Competent authorities in the jurisdiction from which the client's funds originate;
* (c) Competent authorities in the jurisdiction to which the client's funds are destined;
* (d) Correspondent banks, payment processors, or Virtual Asset Service Providers (VASPs, e.g., Binance) where necessary to comply with law or facilitate transactions.

This disclosure is for the purposes of complying with AML/CFT obligations globally.

11. STAFF TRAINING AND AWARENESS

11.1. The Company shall give priority / attention to the periodic training programs to the governing board, management and employees on AML & CFT.

11.2. The training programs must consider the AML & CFT laws of the Republic of South Africa and the recent trends on the subject, as well as the established anti-laundering internal policies and procedures.

11.3. The records of all the training courses carried out should be kept, including the date, names of each of the training participants, hierarchical level and group to which the trainees belong.

11.4. All new staff shall be trained on money laundering and terrorism financing as an entry requirement.

11.5. The Company shall conduct an on-going employee training programme which, at minimum, ensures that members of staff are adequately trained so that they are aware of:

11.5.1. policies and procedures relating to prevention of money laundering and counter terrorist financing, and

11.5.2. the need to monitor all transactions to ensure that no suspicious activity is being undertaken under the guise of transactions.

12. INDEPENDENT REVIEW AND AUDIT

12.1. The AML Policy are subject to periodic independent review, either internally or by an external compliance provider.

12.2. Findings are reported to senior management and the Board, and corrective actions are implemented.

13. COMPANY'S RESERVED RIGHTS

The Company expressly reserves the following rights, which are integral to this Policy:

13.1. To refuse any application for business without providing a reason.

13.2. To terminate any business relationship at any time, with immediate effect, if it suspects involvement in ML/TF/PF or any illicit activity, or for compliance risk management purposes.

13.3. To refuse to process any transaction at any stage, and to reverse any transaction if it is later found to be non-compliant.

13.4. To impose limits, freeze accounts, or require additional conditions on any account.

13.5. To amend this Policy, the RMCP, fees, and any procedures at any time. The revised version will be effective upon publication on the Company's website.

13.6. To rely on third-party providers for CDD or screening, while retaining ultimate responsibility for compliance.

14. NO LIABILITY AND CLIENT INDEMNITY

14.1. The Company shall not be liable for any loss, damage, cost, or expense (including consequential loss) suffered by a client arising from:
* The Company's good faith compliance with any law, regulation, or directive;
* The exercise of its rights under this Policy;
* Any delay, block, suspension, or refusal of a transaction or service;
* The reporting of a suspicious transaction to authorities.

14.2. The client agrees to indemnify and hold the Company harmless from any claims, losses, or liabilities arising from the client's failure to provide accurate information, comply with this Policy, or from the client's involvement in any unlawful activity.

November 2025 – version 1.0