HIGH CAPITAL MARKETS LTD

ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING POLICY

High Capital Markets Ltd is a company registered in Mauritius with Company Number 183353 is regulated by the Financial Services Commission of Mauritius with License number: GB21026331.
Registered Office 6th Floor, Tower 1, Nexteracom Building Ebene Mauritius

Anti-Money Laundering and Counter-Terrorism Financing Policy

This Anti-Money Laundering and Counter-Terrorism Financing Policy (the "Policy") has been prepared to establish the framework for preventing money laundering and terrorism financing within High Capital Markets Ltd (the "Company"), a legal entity incorporated in the Republic of Mauritius under Company Number 183353. The Company is licensed and regulated by the Financial Services Commission, Mauritius, as an Investment Dealer (Full-Service Dealer, excluding Underwriting) under License Number GB21026331.

This Policy forms an integral part of the Company's Terms of Business (the "Terms"), which govern its relationship with Clients. Any capitalised terms used herein but not defined shall carry the meanings assigned to them in the Terms.

The Company is committed to full compliance with all applicable laws and regulations governing the prevention of money laundering and terrorism financing in the Republic of Mauritius (collectively referred to as the "Applicable Regulation"), including but not limited to:

- The Financial Services Act 2007
- The Financial Intelligence and Anti-Money Laundering Act 2002
- The Code on the Prevention of Money Laundering & Terrorist Financing 2012
- Any other relevant legislation, guidelines, and regulatory requirements in force in Mauritius

Client Due Diligence (DD)

Client Due Diligence is a fundamental component of the Company's AML/CFT control framework. The DD process includes, but is not limited to, the following measures:

Identifying and verifying the identity of the Client, as well as their Principal's and any individuals authorized to act on their behalf

Confirming the Client's current residential or business address

Assessing the nature of the Client's business, financial standing, and the role in which they are engaging with the Company

Gathering information regarding the purpose and intended nature of the business relationship

Conducting ongoing monitoring of the business relationship and reviewing Client transactions to ensure consistency with the Company's understanding of the Client and their risk profile

Determining the origin of funds or assets involved in the relationship

Identifying the relationship between the Client and any third-party providing funds

Establishing the Client's source of wealth and estimated net worth, particularly in high-risk relationships or where unusual or potentially suspicious activity is detected

The Company applies DD measures using a risk-based approach in the following circumstances:

Upon the establishment of a business relationship with a Client

In the course of an existing relationship, where:

There are doubts about the accuracy or completeness of previously obtained identification information

The DD information is deemed insufficient

The Client conducts an unusually large transaction or a series of linked transactions

A natural person Client invests more than USD 40,000 (or equivalent in another currency) across one or more accounts

A legal entity Client invests more than USD 40,000 (or equivalent in another currency) across one or more accounts

The Client significantly alters the way they operate their account

There is suspicion of money laundering or terrorism financing involving the Client

The Company shall conduct periodic reviews of existing Client records to ensure that all documents, data, and information obtained through the DD process remain accurate and up to date, with particular attention to higher-risk Clients.

The Company may, at the discretion of the MLRO, request additional documentation or information from the Client as needed to complete or update the DD process.

The MLRO shall exercise reasonable judgment in determining the acceptability of Client DD documentation, considering the legal and regulatory standards of the Client's jurisdiction.

Identification of Natural Persons

When identifying natural persons, the following personal information must be obtained, including but not limited to:

- Full legal name (including any previous names, aliases, or other names used)
- Date and place of birth
- Nationality
- Current residential address
- Occupation, any public office held, and, where applicable, the name of the employer

Acceptable forms of identity documentation typically include:

- Valid passport
- National identity card or its equivalent in the relevant jurisdiction
- Driving license

All identity documents must be current and valid at the time of the Client's application to the Company.

Documents commonly used to verify a Client's residential address include:

- Utility bill
- Dated bank or credit card statement
- Bank reference letter
- Address confirmation issued by a qualified professional

Address verification documents must be issued within six (6) months prior to the Client's application date.

Alternatively, the Company may verify the Client's address through one of the following methods:

- Reviewing a current electoral register
- Using a third-party address verification service
- Conducting a physical visit to the Client's residential address

The Company must confirm, based on the information and documentation provided, whether the natural person Client is acting on their own behalf. If the Client is acting on behalf of a principal, the following additional documentation is required:

- A valid power of attorney authorizing the third party to act on behalf of the principal

- Identity and address verification documents for the principal, as outlined above

Identification of Legal Persons

When the Client is a legal entity, the Company undertakes a series of due diligence measures to ensure the legitimacy of the entity and its representatives. These measures include:

- Verifying the legal existence of the entity
- Assessing the nature of the entity's business to confirm its legitimacy
- Understanding the ownership and control structure of the entity
- Verifying the identity of the entity's principals
- Confirming the identity and authority of any individual acting on behalf of the entity

Identification data for legal persons typically includes:

- Legal name
- Incorporation or registration number
- Date and country of incorporation or registration
- Registered office address and principal place of business (if different)
- Legal form or status of the entity

The documentation required for verification may vary depending on the type of legal entity and its jurisdiction of incorporation. Common requirements include:

- Certificate of incorporation or equivalent document confirming registration under applicable legislation
- Extract from the relevant corporate registry confirming the company's continued existence
- Most recent financial statements or annual report (audited, where available)
- Details of the registered office and principal place of business
- Identification documents for the company's principals, including at least two directors, as outlined in the natural person identification section

The Company also takes reasonable steps to understand the origin and source of funds or assets involved in the business relationship, and to establish the Client's source of wealth. All information obtained must align with the nature and pattern of the Client's transactions.

In accordance with Clause 17C(6) of the Financial Intelligence and Anti-Money Laundering Act 2002, any individual who knowingly provides false or misleading information to a reporting entity in connection with Client due diligence requirements is committing an offence. Upon conviction, such individual may be subject to a fine of up to MUR 500,000 and/or imprisonment for a term not exceeding five years.

Card Verification

Users intending to use payment cards in connection with the Company's services must undergo card verification in accordance with the Company's internal policies.

Sanctions and PEP Screening

The Company conducts thorough screening of all applicants against recognized Sanctions and Politically Exposed Persons (PEP) lists. Both individuals and legal entities are screened at multiple stages:

- During the onboarding process, when an application is submitted
- Manually by the Compliance Officer in response to anti-fraud and AML alerts
- Automatically on a daily basis using scripts that re-check the entire customer database

The screening process is supported by the Company's internal systems, which integrate tools such as World-Check and other official databases. Manual confirmation is conducted using the World-Check search tool.

Risk Assessment

In alignment with international standards and regulatory expectations, the Company has implemented a comprehensive risk-based approach to combat money laundering and terrorist financing. This methodology enables the Company to identify, assess, and manage risks in a manner that ensures proportional and effective mitigation strategies.

By prioritizing risk according to its severity and likelihood, the Company is able to allocate compliance resources, focusing efforts where they are most needed and where potential exposure is greatest. This targeted approach enhances operational efficiency and strengthens the overall integrity of the Company's financial ecosystem.

Key principles of the risk-based approach include:

- **Proportionality**: Preventive measures are scaled according to the level of risk identified, ensuring that high-risk scenarios receive more rigorous scrutiny and control.
- **Efficiency**: Resources-both human and technological-are deployed in a way that maximizes impact and minimizes unnecessary expenditure.
- **Adaptability**: The risk assessment framework is dynamic and regularly updated to reflect emerging threats, changes in customer behavior, and evolving regulatory landscapes.

- **Prioritization**: Risks are ranked and addressed based on their potential to compromise the Company's compliance posture, with the most significant threats receiving immediate and sustained attention.

This approach not only supports regulatory compliance but also reinforces the Company's commitment to ethical business practices and financial transparency.

Transaction Monitoring

Client verification extends beyond identity checks-it also involves continuous analysis of transactional behavior. The Company places strong emphasis on monitoring transaction patterns as a core component of its risk assessment and suspicious activity detection framework.

To support this, the Company utilizes advanced data analysis tools and system functionalities designed to perform a range of compliance-related tasks, including:

- Capturing and filtering transaction data
- Maintaining detailed records
- Managing investigations and case documentation
- Generating and submitting reports as required by applicable regulations

The system also performs daily checks of users against recognized international sanctions lists (e.g., OFAC), aggregates transaction data across multiple parameters, flags users for enhanced scrutiny, and facilitates service denial or case escalation when necessary. Internal communications and statutory reporting are triggered automatically when relevant thresholds or alerts are met.

Case and Document Management

In accordance with the Company's AML/KYC Policy, all client transactions are subject to ongoing monitoring. The Company reserves the right to take appropriate action in response to suspicious activity, including:

- Reporting transactions of a suspicious nature to the relevant law enforcement authorities via the Compliance Officer
- Requesting additional information or documentation from the client to clarify the nature of a transaction
- Suspending or terminating a client's account if there is reasonable suspicion of involvement in illegal activity

This list is not exhaustive. The Compliance Officer is responsible for daily oversight of client transactions and will exercise discretion in identifying and responding to any activity that may pose a risk to the Company's compliance obligations.

Compliance Officer

The Compliance Officer is a designated and authorized individual within the Company responsible for ensuring the effective implementation and enforcement of the AML/KYC Policy. Their responsibilities include:

- Collecting and verifying user identification information
- Establishing and maintaining internal policies and procedures for the completion, review, submission, and retention of all reports and records required under applicable laws and regulations
- Monitoring transactions and investigating any significant deviations from expected activity
- Implementing a records management system for secure storage and efficient retrieval of documents, files, forms, and logs
- Regularly updating the Company's risk assessment framework
- Providing information to law enforcement authorities as required by law

The Compliance Officer is also authorized to liaise directly with law enforcement agencies involved in the prevention of money laundering, terrorist financing, and other illicit activities.

AML/CTF Education and Training

All Company Officers must be fully informed and aware of the following:

- The Company's AML/CTF policies and procedures
- The identity and responsibilities of the Money Laundering Reporting Officer (MLRO)
- The appropriate channels and formats for reporting suspicions of money laundering or terrorism financing
- Their legal obligations under applicable regulations
- The consequences of failing to report suspicious activity, including potential criminal liability
- Emerging trends, techniques, and typologies in money laundering and terrorism financing
- Evolving behaviors and practices among individuals engaged in illicit financial activities

To ensure ongoing competence, Company Officers will receive regular training beyond the information outlined in this Policy. The purpose of this training is to equip them with the

necessary skills and knowledge to fulfill their AML/CTF responsibilities effectively. Training will focus on:

- Understanding the vulnerabilities of the Company's services to money laundering and terrorism financing
- Knowing the due diligence requirements for different categories of clients
- Accurately assessing information to determine whether specific activities or relationships are suspicious
- Identifying and managing suspicious transactions
- Maintaining a high level of awareness and vigilance between training sessions

Training is conducted by the Compliance Officer and scheduled based on a risk-based approach.

However, at minimum, one training session will be held annually. Given the critical role of the MLRO in ensuring the Company's compliance with AML/CTF obligations, the appointed individual will receive additional, specialized training tailored to their responsibilities.