SPEC

www.specmarkets.com

Anti-Money Laundering & Counter-Terrorism Financing (AML/CTF) Policy

Version: 17 Nov 2025

Anti-Money Laundering & Counter-Terrorism Financing (AML/CTF) Policy

Mauritius has established a comprehensive Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) regime aligned with international standards, particularly those set by the Financial Action Task Force (FATF) and the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), of which Mauritius is a member.

In accordance with the Financial Intelligence and Anti-Money Laundering Act (FIAMLA) and the Prevention of Terrorism Act of Mauritius, Spec Capitals Ltd ("Spec") is legally obligated to verify the identity of all clients prior to the opening of a trading account.

By submitting an application form, opening an account, or engaging in transactions with Spec, the client expressly agrees to provide all information, documents, and assistance necessary for the Company to fulfill its AML/CTF obligations.

Spec maintains a strict AML/CTF policy and enforces comprehensive internal procedures designed to detect, prevent, and report any activity related to money laundering or the financing of terrorism. All employees are trained and required to fully understand and comply with the Company's AML/CTF policies and procedures in accordance with applicable laws and international best practices.

All account applications must be reviewed, approved, and accepted by Spec prior to the commencement of any trading activity.

1. Know your Customer (KYC)

1.1. KYC Requirements for Individuals

Where the client is a natural person, the following information shall be collected:

- True name(s) used
- Residential address, post code, telephone number
- Business address
- Date and place of birth

Client identity must be verified using documents, data, or information obtained from a reliable and independent source, or from any other source that Spec reasonably believes can be relied upon to accurately identify and verify the client.

Accordingly, Spec shall verify the client's identity through the submission of one of the following documents:

- Passport
- National Identity Card

- Government ID, such as a Driver's License

The submitted documents must include a clear photograph of the client.

The client's current residential address must be verified by providing one of the following acceptable documents:

- Recent utility bill (phone, gas, electricity)
- Recent Bank or Credit Card statement (photo/scan of a physical letter or PDF of the statement)
- Government-issued Tax Documents

The utility bill, bank or credit card statement must not be older than 3 months from the date of submission.

1.2. KYC Requirements for Corporates

Where the client is not an individual, Spec shall take reasonable measures to identify and verify the client's identity based on the following information:

A. Legal Entity Identification

a) The name, legal form, and proof of existence of the entity, including:
   - Documentation confirming the powers that regulate and bind the entity, and the names of individuals holding senior management positions
   - The registered office address, and where different, the principal place of business

b) Verification that any individual purporting to act on behalf of the entity is duly authorised to do so.

c) Identification and verification of the identity of such authorised individuals.

B. Beneficial Ownership Verification

Spec shall take reasonable, risk-sensitive measures to identify and verify the beneficial owners of the entity. In the case of a legal person, this includes obtaining the following information:

- The identity of the individual with a controlling ownership interest
- The identity of any individual exercising control through other means
- Where no such persons are identified, the identity of the relevant individual holding a senior management position

C. Required Documentation

For legal persons, the following documents shall be collected to verify the information outlined above:

a) Government-issued documentation confirming the legal existence of the business or entity, such as:

- Certified Articles of Incorporation
- Government-issued business license
- Partnership agreement
- Trust deed or instrument

b) Copies of the By-Laws and the latest General Information Sheet, listing directors/ partners, principal shareholders, and any applicable secondary licenses

c) Proof of the principal place of business

d) Proof of business address (e.g., utility bill, lease agreement)

e) Documents confirming the ownership structure, such as:

- Certificate of Directors
- Certificate of Shareholders
- Certificate of Registered Office

Where these are not available, a Certificate of Incumbency detailing the registered address, issued shares, and all directors and shareholders may be provided as an alternative

f) Proof of identity for all directors and shareholders holding more than 10% ownership (e.g., copies of passports or national identity cards)

g) Proof of residential address for the above individuals (e.g., utility bill or bank statement not older than three (3) months)

D. Additional Requirements

Where applicable, Spec may request further information or documentation necessary to comply with relevant Anti-Money Laundering (AML) and Counter-Financing of Terrorism (CFT) obligations.

1.3. Identity Verification and Account Approval

Spec employs a robust client identity verification process that includes:

- Automated ID verification tools to validate document authenticity;
- Sanctions screening tools to check names against global watchlists (e.g., FATF, UN, OFAC, EU, Australian DFAT);
- Manual compliance review for oversight and accuracy.

Spec reserves the right to refuse the processing of any transfer at any stage, should it suspect that the transaction is, in any way, linked to money laundering, terrorist financing, or other

criminal activity. In accordance with applicable laws and regulations, Spec is prohibited from informing clients if they are the subject of a suspicious activity report.

An account will not be opened in the absence of the required identification information. Specifically:

- The client fails to provide the necessary identification;
- Submitted documents are unverifiable or deemed fraudulent;
- The client refuses to supply additional documentation when requested;
- Other factors materially increase the risk of money laundering or terrorism financing, in the view of Spec.

1.4. Sanction Lists

All individuals and entities engaging with Spec will be screened against applicable sanctions lists. These checks will be conducted at the time of onboarding and periodically thereafter in accordance with updated sanctions lists.

Spec screens all clients and transactions against multiple international sanctions lists, including but not limited to:

- The United Nations Consolidated Sanctions List;
- The Financial Action Task Force (FATF) high-risk jurisdictions;
- The Office of Foreign Assets Control (OFAC);
- The European Union and Australian sanctions lists.

If a client is identified as being from, or associated with, a sanctioned country or jurisdiction, Spec will not proceed with account opening. In the case of existing clients found to be in breach of applicable sanctions, their accounts will be subject to immediate termination.

2. Record Keeping

Spec will maintain records in accordance with applicable Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) regulations, including but not limited to the Financial Action Task Force (FATF) Recommendations, the European Union Anti-Money Laundering Directives, the United Nations Security Council Resolutions, the U.S. Office of Foreign Assets Control (OFAC) guidelines, and all relevant local laws and regulations in Mauritius and other applicable jurisdictions.

2.1. Transaction Records

All records of financial transactions conducted by or on behalf of clients must be maintained and securely stored for seven (7) years from the date of the transaction.

2.2. Client Identification and Due Diligence Records

Client due diligence (CDD) documentation, including but not limited to identification documents, corporate registration records, beneficial ownership information, and business correspondence,

must be retained for at least five (7) years following the termination of the business relationship or closure of the account.

2.3. Ongoing Obligations

If required by applicable law or in connection with investigations or regulatory obligations, retention periods may be extended beyond the minimum periods noted above, up to a maximum of ten (10) years.

2.4. Data Protection

Spec recognises its obligations as a data controller under the EU General Data Protection Regulation (GDPR) and commits to the lawful, fair, and transparent processing of personal data.

Retention of personal data under this policy is based on the lawful basis of compliance with a legal obligation (Article 6(1)(c) GDPR), specifically obligations imposed under AML/CTF regulations.

Spec ensures that:

- Only data that is necessary to meet AML/CTF obligations is retained
- Data is not kept for longer than is legally required
- Once the retention period has expired, data will be securely deleted, destroyed, or anonymised

All retained records are stored securely and access is restricted to authorised personnel only. Appropriate technical and organisational measures are implemented to prevent unauthorised access, disclosure, alteration, or destruction.

> Clients are informed of the retention of their personal data, including the legal basis and retention periods, through Spec's Privacy Policy and onboarding documentation.

3. Suspicious Activity & Reporting Obligations

Spec has a legal obligation to identify and report any transaction that appears suspicious or inconsistent with a client's known profile, business activities, or stated source of funds.

As part of the Client's relationship with Spec, the Client agrees to:

- Provide accurate and truthful information during account registration and verification;
- Notify the Company of any changes to identification details, source of funds, or ownership structure (if applicable);
- Avoid using the trading account for unlawful or fraudulent activity, including transactions on behalf of others without disclosure;
- Comply with all KYC/AML requirements, including providing documentation or explanations when requested.

If Spec reasonably suspects that the Client's transactions or account activity may involve money laundering, terrorism financing, or other financial crime:

- The Company is legally required to report any suspicious activity to the Financial Intelligence Unit (FIU) of Mauritius, in accordance with the Financial Intelligence and Anti-Money Laundering Act (FIAMLA) and other applicable legislation;
- The Client's account may be frozen, restricted, or closed without prior notice, where permitted by law;
- Additional documentation or clarification may be requested;
- The Company may be required to retain copies of the Client's records and transactions for extended periods.

Spec is prohibited by law from notifying the Client if a report has been filed with authorities, in accordance with Mauritius anti–tipping-off laws.

Spec may be legally required to share Client account or transaction details with regulatory or law enforcement authorities if mandated to do so. This includes complying with court orders, subpoenas, or lawful requests from the FIA or other relevant authorities.

4. Ongoing monitoring of transactions

As part of Spec's commitment to preventing money laundering and other financial crimes, the Company continuously monitors Client transactions to ensure alignment with the Client's profile, declared source of funds, and stated purpose of the trading account.

- The Client acknowledges and agrees that:
- Trading activity, deposits, and withdrawals may be reviewed on an ongoing basis;
- Additional information or documentation may be requested to support certain transactions;
- The Client is expected to ensure activity remains consistent with the stated purpose of the account and declared financial profile;
- Spec may delay, restrict, or decline transactions that appear unusual, inconsistent, or raise reasonable suspicion.

The Company may conduct further checks or request clarification if it detects:

- Unusually large or frequent transfers;
- Transactions inconsistent with your previous activity or stated income;
- Use of multiple third-party accounts or undisclosed payment methods;
- Sudden changes in trading behaviour or volume;
- Activity involving high-risk or sanctioned jurisdictions.

To maintain a secure trading environment, the Client agrees to:

- Respond promptly to compliance-related requests;
- Maintain accurate and up-to-date account information, including identity and source of funds documentation;
- Avoid using the trading account for third-party benefit without disclosure.

All monitoring is conducted in accordance with applicable privacy and data protection laws. The Client will not be notified if a suspicious activity report is made, in compliance with anti–tipping-off laws.

5. Internal controls and compliance programs

Spec is committed to maintaining a robust compliance and internal control framework designed to prevent and detect money laundering, terrorism financing, and other forms of financial crime. We apply global best practices and follow the legal obligations set out in the Financial Intelligence and Anti-Money Laundering Act (FIAMLA) of Mauritius, the Prevention of Terrorism Act, and international standards established by the Financial Action Task Force (FATF) and the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG).

To safeguard our clients and the financial system, Spec has implemented the following key controls:

- **Client Due Diligence (CDD)**: All clients must undergo identity verification and provide documents such as proof of identity, address, and source of funds before being approved for trading.
- **Enhanced Due Diligence (EDD):** Additional scrutiny is applied to high-risk clients, including those from high-risk jurisdictions or with complex structures.
- **Sanctions Screening**;
- **Ongoing Monitoring;**
- **Automated Surveillance Systems**: Spec uses risk-based monitoring tools to identify red flags and potential violations of AML/CTF policies.
- **Suspicious Activity Reporting**: Where required, reports are filed with the Financial Intelligence Unit (FIU) of Mauritius. Clients will not be notified when such reports are made, in line with anti–tipping-off provisions under the Financial Intelligence and Anti-Money Laundering Act (FIAMLA).
- **Staff Training & Awareness**: All employees receive regular AML/CTF training to ensure awareness of compliance obligations and proper handling of red flag indicators.
- **Periodic Review of Client Profiles**: Client data is reviewed periodically and updated as needed to ensure ongoing compliance and suitability.

Spec maintains a zero-tolerance policy for the misuse of its services for illicit purposes. Any activity that raises concerns will be subject to internal investigation, potential account suspension, and reporting to the relevant authorities as required by law.

6. Client Responsibilities

To ensure compliance with international Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) laws, all Clients are required to fulfill certain responsibilities. These include:

- Providing accurate and up-to-date identity and residential documents during account registration and upon request;
- Immediately notifying Spec of any changes in personal details, including contact, residency, employment, or financial status;
- Using only bank accounts or payment methods registered in the Client's name for deposits and withdrawals;
- Avoiding third-party transactions that conceal the true ownership or origin of funds;
- Responding promptly and completely to compliance inquiries or document requests;
- Refraining from suspicious, illegal, or abusive trading activity;
- Using the trading platform for lawful purposes consistent with the Client's financial profile and trading objectives;
- Cooperating with enhanced due diligence checks where applicable;
- Understanding that Spec may restrict or terminate access to services if documentation or behaviour is inconsistent with legal or internal requirements;
- Reviewing all compliance disclosures and risk warnings before initiating trading activity.