EveryTrade24

Policies and Procedures Manual – Everytrade 24 LTD

Global Business Licence (GBL) – Licence No. GB25204986
Last Update: October 2025

Table of Contents

Definitions

- "**Access Person**" includes any supervised person who has access to non-public information regarding any clients' purchase or sale of securities, or non-public information regarding the portfolio holdings of any fund the adviser or its control affiliates manage; or is involved in making securities recommendations to clients, or has access to such recommendations that are non-public. All of the Company's directors, officers, and partners are presumed to be access persons.
- "**Company**" means Everytrade24 Ltd and vice versa.
- A "**Covered Security"** is "being considered for purchase or sale" when a recommendation to purchase or sell the Covered Security has been made and communicated and, with respect to the person making the recommendation, when such person seriously considers making such a recommendation.
- "**Conflict of Interest**": for the purposes of this document, a "conflict of interest" will be deemed to be present when an individual's private interest interferes in anyway, or even appears to interfere, with the interests of the Company as a whole.
- "**Covered Security**" means any stock, bond, future, investment contract or any other instrument that is considered a "security" under the Act. Additionally, it includes options on securities, on indexes, and on currencies; all kinds of limited partnerships; foreign unit trusts and foreign mutual funds; and private investment funds, hedge funds, and investment clubs.
- "**Covered Security**" does not include direct obligations of the U.S. government; bankers' acceptances, bank certificates of deposit, commercial paper, and high quality short-term debt obligations, including repurchase agreements; shares issued by money market funds; shares of open-end mutual funds that are not advised or sub-advised by the Company; and shares issued by unit investment trusts that are invested exclusively in one or more open-end funds, none of which are funds advised or sub-advised by the Company.
- "**GBL**" refers to Global Business License issued by the FSC
- "**ID License**" refers to an Investment Dealer Full-Service Dealer, excluding Underwriting license
- **"IDL**" or **'ID'** refers to Registered Investment Dealer
- "**Investment personnel**" means: (i) any employee of the Company or of any company in a control relationship to the Company who, in connection with his or her regular functions or duties, makes or participates in making recommendations regarding the purchase or sale of securities for clients.
- **"FSC"** refers to the Mauritius Financial Services Commission
- "**Purchase or sale of a Covered Security**" includes, among other things, the writing of an option to purchase or sell a Covered Security.
- **"Reportable security"** The Rule considers all securities reportable except for the following:
  Direct obligations of the Government of the United States;
  Bankers' acceptances, bank certificates of deposit, commercial paper and high-quality short-term debt instruments, including repurchase agreements;
  Shares issued by money market funds;
  Shares issued by open-end funds other than reportable funds; and
  Shares issued by unit investment trusts that are invested exclusively in one or more open-end funds.
- "**Supervised Persons**" means directors, officers, and partners of the adviser (or other persons occupying a similar status or performing similar functions); employees of the adviser; and any other person who provides advice on behalf of the adviser and is subject to the adviser's supervision and control.

1. Policy Statement

It is unlawful for an IDL to provide investment advice unless the IDL has adopted and implemented written policies and procedures reasonably designed to prevent violation of regulations and rules by the IDL or any of its supervised persons. The rule requires dealers to consider their fiduciary and regulatory obligations under the FSC and regulations and rules, and to formalize policies and procedures to address them. This document is provided as documentation of those policies and procedures.

Reviews of these policies and procedures are to be conducted on an annual basis at a minimum. Interim reviews may be conducted in response to significant compliance events, changes in business arrangements, and regulatory developments.

Company will maintain copies of all policies and procedures that are in effect or were in effect at any time during the last seven years.

a) Compliance Officer ('CO') Appointment

The person herein named "Compliance Officer" is stated to be competent and knowledgeable regarding the applicable rules and regulations and is empowered with full responsibility and authority to develop and enforce appropriate policies and procedures for the company, Everytrade24 Ltd (the "**Company**"). The CO has a position of sufficient seniority and authority within the organization to compel others to adhere to the compliance policies and procedures.

2. Fiduciary Statement

a) Background

The Company holds a GBL issued by the FSC on 1st of September 2025 as well as, an ID License, granted by the FSC on the same date.

An ID has an affirmative duty to act in the best interests of its clients and to make full and fair disclosure of all material facts to the exclusion of any contrary interest. Generally, facts are "material" if a reasonable person would recognize them as relevant to a decision to be made, as distinguished from an insignificant, trivial, or unimportant detail. In other words, it is a fact, the suppression of which would reasonably result in a different decision. The duty of addressing and disclosing conflicts of interest is an ongoing process and as the nature of an investment dealer's business changes, so does the relationship with its clients.

b) Company Statement

The Company is an IDL, regulated by the FSC under the license number: GB25204986

As an investment dealer, the Company owes its clients specific duties of a fiduciary nature:

- Provide advice that is suitable for the client;
- Give full disclosure of all material facts and any potential conflicts of interest to clients and prospective clients;
- Serve with loyalty and in utmost good faith;
- Exercise reasonable care to avoid misleading a client; and
- Make all efforts to ensure best execution of transactions.

The Company seeks to protect the interest of each client and to consistently place the client's interests first and foremost in all situations. It is the belief of the Company, as an investment dealer, that its policies and procedures are sufficient to prevent and detect any violations of regulatory requirements as well as, the Company's own policies and procedures.

3. Code of Ethics Statement

a) Background

In accordance with regulations, the Company has adopted a code of ethics (herein described under section 3) to:

- Set forth standards of conduct expected of advisory personnel (including compliance with securities laws); and
- Safeguard material non-public information about client transactions.

b) Introduction

As an ID, the Company has an overarching fiduciary duty towards its clients, whose interests come first. The Company has an obligation to uphold that fiduciary duty and see that its personnel do not take inappropriate advantage of their positions and the access to information that comes with their positions.

The Company holds its directors, officers, dealers, and employees accountable for adhering to and advocating the following general standards to the best of their knowledge and ability:

1. The Company and all its group entities shall observe and comply with all relevant laws wherever they operate.
2. The Company and all its group entities shall observe and comply with the spirit as well as the letter of the regulations prescribed by the FSC.
3. The Company and all its group entities shall cooperate with all responsible authorities in the jurisdictions where it operates.
4. The Company and all its group entities shall act in a manner which recognizes that integrity and responsibility are essential to win and maintain the confidence of the Company and all its group entities of the public in all aspects of the fund industry.
5. The Company and all its group entities shall conduct their businesses in a professional manner and in accordance with sound business practice.
6. The Company and all its group entities shall ensure that their staff are thoroughly and appropriately trained, knowledgeable and competent in all aspects of the fund industry which are relevant to the proper performance of their duties and responsibilities.
7. The Company and all its group entities shall ensure that it will obtain any applicable authorisations and license in any relevant jurisdiction before engaging in active marketing of Company Products/Activities in those jurisdictions unless the customers from those jurisdictions reach out to the Company without any solicitation form the Company. The Board shall take a decision on these situations on a case to case basis.
8. The Company and all its group entities shall respect and preserve the confidentiality of their clients and investors in their funds.
9. The Company and all its group entities shall not use information provided by clients which has not been made public for their own or others benefit, as this may amount to insider dealing.
10. The Company and all its group entities shall ensure that the overriding principle in carrying out its activities is the benefit and interest of investors.
11. The Company and all its group entities shall not issue any misleading advertisements or intrude upon the privacy of the public through door-to-door canvassing, either directly or through third party brokers, or other similar methods or through illegal and unethical methods. The Company shall maintain and advertising policy for annual review by the Board.

12. The Company and all its group entities shall provide investors with all requisite documentation promptly in accordance with their stated intentions. The Company's website includes all the legal documents, reference to FAQs on the Company for ease of client's access.
13. The Company and all its group entities shall abide by all policies and statements of intention stated in their offering documentation and shall ensure that investors and potential investors are given adequate warning of any proposed changes of intention or policy.
14. The Company and all its group entities shall not engage in any professional conduct involving dishonesty, fraud, deceit or misrepresentation or commit any act that reflects adversely on its honesty, trustworthiness or professional competence.
15. The Code of Ethics, described herein, will be binding on the directors, the dealers, all officers, advisers, managers, representatives and employees of the Company and all its group entities.
16. Professional misconduct in the nature of misrepresentation and fraudulent, dishonest or misleading conduct by any director, dealer, officer, adviser, manager, representative or employee of the Company and all its group entities will result in disciplinary action and prosecution where applicable.
17. Failure to comply with the Company's Code of Ethics may result in disciplinary action, up to and including termination of agreement/employment. Such action shall be determined by the Board Members. Should a Director be involved in the breach, then the latter will not be allowed to vote in the matter under discussion.

4. Prohibited Purchases and Sales

a) Insider Trading

Illegal insider trading refers generally to buying or selling a security, in breach of a fiduciary duty or other relationship of trust and confidence, while in possession of material, non-public information about the security. Information is material if 'there is a substantial likelihood that a reasonable shareholder would consider it important, in making an investment decision. Information is non-public if it has not been disseminated in a manner making it available to investors generally.

The Company strictly prohibits trading personally or on the behalf of others, directly or indirectly, based on the use of material, non-public or confidential information. The Company additionally prohibits the communicating of material non-public information to others in violation of the law. Employees/Officers who are aware of the misuse of material non-public information should report such to the data protection officer. This policy applies to all of the Company's directors, employees, officers and associated persons without exception.

The Board shall collect and maintain a list of each access person's personal securities owned. The CO shall review the summaries for inappropriate transactions and report them to Board. Access persons report their personal securities' transactions on at least a quarterly basis and annually thereafter.

5. Prohibited Activities

a) Conflicts of Interest Policy

The Company has an affirmative duty of care, loyalty, honesty, and good faith to act in the best interest of its clients. All supervised persons[1] must refrain from engaging in any activity or having a personal interest that presents a "conflict of interest."

[1] "Supervised Persons" means directors, officers, and partners of the Company (or other persons occupying a similar status or performing similar functions); employees of the Company; and any other person who provides advice on behalf of the Company and is subject to the Company's supervision and control.

A conflict of interest may arise if the supervised person's personal interest interferes, or appears to interfere, with the interests of the Company or its clients. A conflict of interest can arise whenever a supervised person takes action or have an interest that makes it difficult for him/her to perform his/her duties and responsibilities for the Company honestly, objectively and effectively.

While it is impossible to describe all of the possible circumstances under which a conflict of interest may arise, listed below are situations that most likely could result in a conflict of interest and that are prohibited under the Company's policies:

- Access persons may not favor the interest of one client over another client (e.g., larger accounts over smaller accounts, accounts compensated by performance fees over accounts not so compensated, accounts in which employees have made material personal investments, accounts of close friends or relatives of supervised persons). This kind of favoritism would constitute a breach of fiduciary duty; and
- Access persons are prohibited from using knowledge about pending or currently considered securities transactions for clients to profit personally, directly or indirectly, as a result of such transactions, including by purchasing or selling such securities.

- Access persons are prohibited from recommending, implementing or considering any securities transaction for a client without having disclosed any material beneficial ownership, business or personal relationship, or other material interest in the issuer or its affiliates, to the Board. If the Board deems the disclosed interest to present a material conflict, the investment personnel may not participate in any decision-making process regarding the securities of that issuer.

  Pursuant to paragraph 3.4.1 of the Anti-Money Laundering and Countering the Financing of Terrorism Handbook issued by the FSC in January 2020 (the "**FSC Handbook**"), the circumstances of the Company may be such that, due to the small number of employees, the CO holds functions in addition to his/her functions of the CO as prescribed under Mauritius laws and regulations, or is responsible for other aspects of the Company's operations. Where this is the case, the Company must ensure that any conflicts of interest between the responsibilities of the CO's role and those of any other functions are identified, documented and appropriately managed. The CO however should be independent of the core operating activities of the Company and should not be engaged in soliciting business. Such details shall be disclosed in the Interest Register of the Company.

  The Company and all its directors, dealers, officers will act in the best interest of clients.

- An interests register will be kept by the Company and updated regularly.

- The personal interests of a director, or persons closely associated with the director, must not take precedence over those of the Company and participants.

- A director should make his/her best effort to avoid conflicts of interest or situations where others might reasonably perceive there to be a conflict of interest.

- Full and timely disclosure, in writing, of any conflict, or potential conflict relating to directors and management must be made known to the Board.

- Where an actual or potential conflict does arise, on declaring their interest and ensuring that it is entered on the Register of interests of the Company, a director can participate in the debate and/or indicate their vote on the matter, although such vote would not be counted. The director must give careful consideration in such circumstances to the potential consequences it may have for the Board and the Company.

- Directors should recognise that their duty and responsibility as director is always to act in the interests of the Company and not any other party.

- Directors and officers must treat confidential matters relating to the Company, learned in his/her capacity as director/officer, as strictly confidential and must not divulge them to anyone without the authority of the Board. The Board must consider each such request on its merits and on a case-by-case basis.

b) Managing Conflicts of Interest

It is vital for the Company which will be carrying out more than one regulated activity vis-a-vis its clients, to identify and manage any conflict of interest that may arise in the course of providing such services.

Conflict of interest may arise between the Company's interest and that of its client and between the interests of one client and another. The Company shall endeavour to manage these conflicts of interest by:

- Establishing well defined Chinese walls segregating the Management Functions and Operational Teams and Advisory Functions;
- Independent oversight;
- Disclosure;
- Declining to provide the service.

Any conflict-of-interest situation or potential conflicts' situation should be reported immediately (within 5 days) to the relevant Committee who shall escalate it to the Board of the Company.

c) Gifts and Entertainment

Supervised persons should not accept inappropriate gifts, favors, entertainment, special accommodations, or other things of material value that could influence their decision-making or make them feel beholden to a person or firm. Similarly, supervised persons should not offer gifts, favors, entertainment or other things of value that could be viewed as overly generous or aimed at influencing decision-making or making a client feel beholden to the Company or the supervised person.

No supervised person may receive any gift, service, or other thing of more than de minimis value from any person or entity that does business with or on behalf of the ID. No supervised person may give or offer any gift of more than de minimis value to existing clients, prospective clients, or any entity that does business with or on behalf of the ID without written pre-approval by the Board. The annual receipt of gifts from the same source valued at $250.00 or less shall be considered de minimis. Additionally, the receipt of an occasional dinner, a ticket to a sporting event or the theater, or comparable entertainment also shall be considered to be of de minimis value if the person or entity providing the entertainment is present. All gifts, given and received, will be recorded in a log to be signed by the supervised person and a Director and kept in the supervised person's file.

No supervised person may give or accept cash gifts or cash equivalents to or from a client, prospective client, or any entity that does business with or on behalf of the adviser.

Bribes and kickbacks are criminal acts, strictly prohibited by law. Supervised persons must not offer, give, solicit or receive any form of bribe or kickback.

d) Political and Charitable Contributions

Supervised persons that make political and/or charitable contributions, in cash or services in excess of USD 10,000 (or equivalent or more than MUR 500,000), must report each such contribution to the Board. This information will be compiled and reported thereon as required under relevant regulations. Supervised persons are strictly prohibited from considering the ID's current or anticipated business relationships as a factor in soliciting political or charitable donations. This policy becomes enforceable only if a government or state owned entity is a client of the Company.

e) Confidentiality

Supervised persons shall respect the confidentiality of information acquired in the course of their work and shall not disclose such information, except when they are authorized or legally obliged to disclose the information. They may not use confidential information acquired in the course of their work for their personal advantage. Supervised persons must keep all information about clients (including former clients) in strict confidence, including the client's identity (unless the client consents), the client's financial circumstances, the client's security holdings, and advice furnished to the client by the Company.

f) Service on Board of publicly traded companies

Supervised persons shall not serve on the board of directors of publicly traded companies whether in Mauritius or elsewhere unless prior authorization has been received from the Board of the Company in writing. Any such approval may only be made if it is determined that such board service will be consistent with the interests of the clients and of the Company, and that such person serving as a director will be isolated from those making investment decisions with respect to such Company by appropriate procedures. A director of a private company may be required to resign, either immediately or at the end of the current term, if the Company goes public during his or her term as director.

g) Relationships with Regulatory Bodies

Officers may come into contact with representatives from regulatory bodies during the course of their work. Officers are expected to deal with the Regulators in a cooperative manner and must comply with any disclosure obligations in a prompt manner. Officers shall pay attention to Part III – Financial Crimes described in The Financial Crimes Commission Act 2023 and ensure that they are not engaged in any acts that can fall under the definition of bribery, influence peddling ('trafic d'influence'), corruption, money laundering, fraud, financing drug dealing activities, conspiracy, abetting, make/possess/supply articles connected to the abovementioned offences, terrorism financing and proliferation.

6. Compliance Procedures

a) Compliance with Laws and Regulations

All supervised persons of the Company must comply with all applicable laws. Specifically, supervised persons are not permitted, in connection with the purchase or sale, directly or indirectly, of a security held or to be acquired by a client:

- To defraud such client in any manner;
- To mislead such client, including making any statement that omits material facts;
- To engage in any act, practice or course of conduct which operates or would operate as a fraud or deceit upon such client;

- To engage in any manipulative practice with respect to such client; or
- To engage in any manipulative practice with respect to securities, including price manipulation.

Breach of the above shall be considered by the Board of Directors fairly and where applicable, sanctioned.

b) Personal Securities Transactions Procedures and Reporting

A. Pre-Clearance

All supervised persons must follow the following procedures before executing any personal trades:

1. Pre-clearance requests must be submitted by the requesting supervised person to the Board or the appropriate supervisor in writing. The request must describe in detail what is being requested and any relevant information about the proposed activity.
2. The Board/Supervisor will respond in writing to the request as quickly as practical, either giving an approval or declination of the request, or requesting additional information for clarification.
3. Pre-clearance authorizations expire 48 hours after the approval, unless otherwise noted by the Board/Supervisor on the written authorization response.
4. Records of all pre-clearance requests and responses will be maintained by the Board for monitoring purposes and ensuring the Code of Ethics is followed.

B. Pre-Clearance Exemptions

The pre-clearance requirements of this section shall not apply to:

1. Purchases or sales affected in any account over which the access person has no direct or indirect influence or control.
2. Purchases which are part of an automatic investment plan, including dividend reinvestment plans.
3. Purchases effected upon the exercise of rights issued by an issuer pro rata to all holders of a class of its securities, to the extent such rights were acquired from such issuer, and sales of rights so acquired.
4. Acquisition of covered securities through stock dividends, dividend reinvestments, stock splits, reverse stock splits, mergers, consolidations, spin-offs, and other similar corporate reorganizations or distributions generally applicable to all holders of the same class of securities.
5. Open end investment company shares other than shares of investment companies advised by the Company or its affiliates or sub-advised by the Company
6. Certain closed-end index funds.
7. Unit investment trusts.
8. Exchange traded funds that are based on a broad-based securities index.
9. Futures and options on currencies or on a broad-based securities index.

7. Policy review and Acknowledgement

a) Initial Certification

The Company is required to provide all supervised persons/officers with a copy of this policy. All supervised persons are required to certify in writing that they have: (a) received a copy of this policy; (b) read and understood all provisions of this policy; and (c) agree to comply with the terms of this policy.

b) Acknowledgement of Amendments

The Company must provide supervised persons with any amendments to this policy and supervised persons must submit a written acknowledgement that they have received, read, and understood the amendments to this policy.

The CO shall maintain records of these acknowledgements.

c) Annual Review

This Policy shall be subject to an annual review by the Board for its adequacy and effectiveness. Such review shall be tracked and kept on record. Any amended policies shall be approved by the Board via minutes or resolutions before implementation.

8. Training and education

The Company shall arrange for necessary trainings or educational exchanges or webinars for officers and supervised persons regarding this policy periodically, such period and method of education shall be determined by the Board. All supervised persons are required to mandatorily fulfill these training / webinars / educational exchange programs, read any applicable materials and acknowledge their training in writing via an attendance sheet.

9. Recordkeeping

The Company shall ensure that the following records are maintained in a readily accessible place:

- A copy of this policy and other such policies that have been in effect at any time during the past seven years;
- A record of any violation of the policy and any action taken as a result of such violation for seven years from the end of the fiscal year in which the violation occurred;
- A record of all written acknowledgements of receipt of the policy and amendments for each person who is currently, or within the past seven years was a supervised person. These records must be kept for seven years after the individual ceases to be a supervised person of the Company;
- Holdings and transactions reports made pursuant to the policy, including any brokerage confirmation and account statements made in lieu of these reports;
- A list of the names of persons who are currently, or within the past seven years were, access persons;
- A record of any decision and supporting reasons for approving the acquisition of securities by access persons in initial public offerings and limited offerings for at least seven years after the end of the fiscal year in which approval was granted.
- The establishment of a business relationship, for at least seven years from the date on which the business relationship is terminated;
- A transaction which is concluded, for at least 7 years from the date on which that transaction is concluded; and
- Reports made by and to the MLRO, for at least 7 years from the date on which the report is made. Such report shall be confidential and maintained by the MLRO or in his/her absence by the DMLRO.

The Company must further keep record of:

- the identity and address of the investor/client;
- if the customer is acting on behalf of another person:
- the identity and address of the person on whose behalf the customer is acting; and
- the customers authority to act on behalf of that other person;
- if another person is acting on behalf of the investor/client:
- the identity and address of that other person; and
- that other person's authority to act on behalf of the investor;
- the nature of the business relationship or transaction;
- the intended purpose of the business relationship; and
- the source of funds which the prospective client is expected to use in concluding transactions in the course of the business relationship;
- in the case of a transaction:
    - the amount involved and the currency in which it was denominated;
    - the date on which the transaction was concluded;
    - the parties to the transaction;
    - the nature of the transaction; and
    - business correspondence;
    - if the Company provides account facilities, the identifying particulars of all accounts at the Company that are related to the transaction;
    - any document or copy of a document obtained by the Company in order to verify a person's identity.

Further, the Company must keep records of all trainings provided in relation to anti money laundering and countering of financing of terrorism and proliferation and bribery .

Transactional records and or documents are kept at the Company's registered office. Records should be sufficient to provide adequate evidence to the relevant local authorities to conduct their investigations. The supervised persons shall make sure that records are shared with the Company Administrator in a complete set, transparently, in a timely manner for appropriate record keeping processes to be fulfilled.

10. Client instructions/ onboarding described

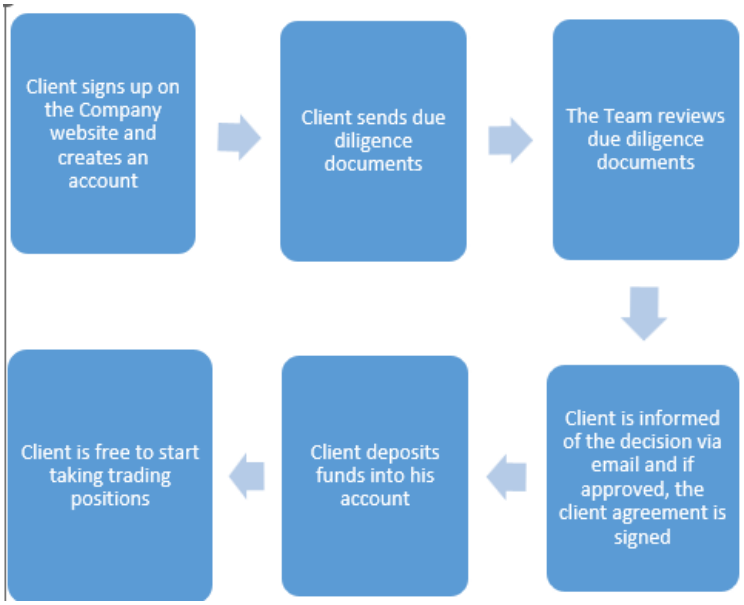
Process:

i. Client initiates contact via Company's website either via chat options or via the 'sign up' option or via the 'contact us' tab.
ii. After clarifying any inquiries (if applicable, the client completes the onboarding form and submits same on electronically by email.
    - The application includes the requirement for the client to upload his/her due diligence documents.
    - Such documents are verified in terms of validity.
iii. The Company also screens the name of the client against international databases of PEPs, sanctions, enforcement actions, adverse media among others.
iv. The standard due diligence documents and information that should be sought from clients are as follows:
    1. Passport copy
    2. Proof of address (in the form of utility bill, or bank statements or bank reference letter among others
    3. Bank details
    4. Contact Details

5. Profile Information
6. Source of Funds Declaration information

v. The Onboarding Team then verifies the application for completeness and proceeds with the automatic risk assessment of the customer.
vi. Based on the risk category of the customer (that is for High-Risk Customers), the application is referred to a Board Member for approval.
vii. Any one director shall approve/reject any client is deemed to be high risk;
viii. The decision for onboarding is then automatically delivered to the client by email.
ix. If approved the client's online account is activated and client is informed to fund the account.

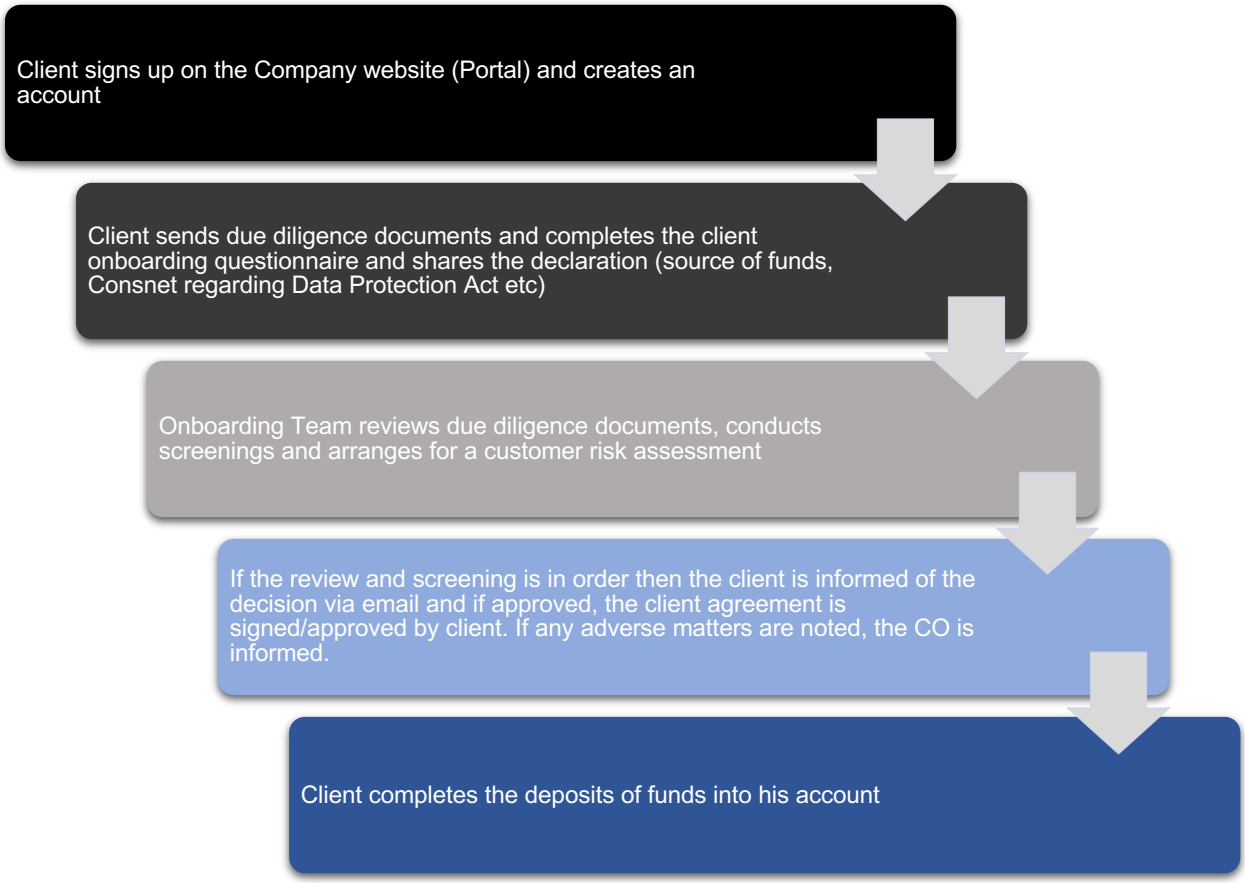
Diagram 1: Client onboarding flow chart



a) Due Diligence Checks and Records

Due diligence checks shall be conducted by the Team. In addition, the Company confirms that, all supporting documentation will be kept at its registered office address.

Diagram 1: Client onboarding flow chart



11. Advertising Policy

The Company's Board of Directors shall be responsible for approving all Company advertising and ensuring it is in compliance with jurisdictional regulations. No advertisement shall be distributed without the Board Members' unanimous approval.

a) Compliance Requirements:

Pursuant to certain rules and regulations, an advertisement may not:

- Use or refer to testimonials (which include any statement of a client's experience or endorsement);
- Mislead clients using misrepresentations or exaggerations;

- Refer to past, specific recommendations made by the adviser that were profitable, unless the advertisement sets out a list of all recommendations made by the adviser within the preceding period of not less than one year, and complies with other, specified conditions;

- Represent that any graph, chart, formula, or other device can, in and of itself, be used to determine which securities to buy or sell, or when to buy or sell such securities, or can assist persons in making those decisions, unless the advertisement prominently discloses the limitations thereof and the difficulties regarding its use; and
- Represent that any report, analysis, or other service will be provided without charge unless the report, analysis or other service will be provided without any obligation whatsoever.

An advertisement shall include any notice, circular, letter, Email or other written communication (including any social media communications such as Facebook messaging, Twitter feeds, online blogs or any other internet communication) addressed to more than one person, or any notice or other announcement in any publication or by radio or television, which offers (1) any analysis, report, or publication concerning securities, or which is to be used in making any determination as to when to buy or sell any security, or which security to buy or sell, or (2) any graph, chart, formula, or other device to be used in making any determination as to when to buy or sell any security, or which security to buy or sell, or (3) any other investment advisory service with regard to securities.

b) Social Media Policy

The following websites are considered Social Media sites: 1) Facebook; 2) Twitter; 3) LinkedIn; 4) Instagram; 5) Reddit; 6) YouTube; 7) Blogs

The Company has adopted the following policies and procedures concerning the usage of social media websites by its supervised persons:

1) All social media site usage is considered correspondence and/or advertising by the Company.
2) All usage and posting to these sites must be monitored and approved by the Company's CO.
3) The Company requires that all social media usage and posts must be retained and archived.
4) Supervised persons are not permitted to post any specific investment recommendations to social media.
5) When investment recommendations are discussed on any platform, there will be disclosures put in place.

12. Accuracy of Disclosures Made to Clients and Regulators

The Board is responsible for the accuracy of all disclosures made to clients, and regulators. Where third party disclosure documents are involved, the Company will ensure that the disclosures have been tabled to the Board for approval.

a) Account Statements

The Company will review client account statements to ensure their accuracy. All client account statements will be stored electronically. Customer should refer to their statements on the client portal and trading platform.

b) Advertisements

All advertisements are reviewed to ensure their accuracy, specifically in regards to any performance claims. The Board will review all performance calculations contained in advertisements to ensure performance was accurately calculated.

c) Privacy Policy

The privacy policy statement is given to clients at the initial onboarding stage. A copy of the privacy policy is available on the Company's website.

13. Information Security & Cybersecurity

The Company has taken extensive measures to safeguard the privacy and integrity of the information that it gathers, stores, and archives during its normal business practices. Computer security measures have been instituted where applicable including passwords, backups, and encryption. All employees/officers are informed and instructed on various security measures including the non-discussion and/or sharing of client information, always removing client files from desktops or working areas that cannot be locked or secured, and proper storage of client securities files in locked files or other secured location. The Company maintains physical, electronic, and procedural safeguards to guard nonpublic personal information.

In addition to electronic and personnel measures, the Company has implemented reasonable physical security measures at our office locations to prevent unauthorized access to our facilities.

a) Third Party Vendors

The Company uses various methods to store and archive client files and other information. All third-party services or contractors used have been made aware of the importance the Company places on both Company and client information security.

The Company utilizes various third-party vendors for its business activities. The Company has collected, reviewed and maintains the privacy policies and cybersecurity policies of all its third-party vendors.

b) Cybersecurity Risks and Controls

The Company periodically assess the nature, sensitivity and location of information it collects and maintains. As a financial institution, the Company understands our business is vulnerable to cybersecurity incidents. The Company has put tools in place to mitigate these risks including but not limited to: anti-virus software, firewalls, and using unique passwords on computers, documents and third-party technology systems used.

The Company recognizes that employees'/officers' emails are susceptible to potential hacks or malicious phishing attempts. To avoid these events, all employees/officers are required to use 2-factor authentication for email logins.

The Company utilizes a cloud-based drive that is backed-up daily and monitored to prevent data loss.

c) Access Control Policy

Company's employees/Officers are limited to viewing and sharing files on both internal and third-party systems that are only relevant to their roles. Upon termination of an employee, there will be an immediate termination of access rights to all systems and offices.

d) Mobile Device Security

Company's employees utilize their personal mobile phone devices for e-mail management while away from their main offices. The Company's employees, when employed, will be required to have 2-step authorization on their email accounts and should only log in to their email on a trusted device. Employees are encouraged to enable passwords on their mobile devices.

If employees misplace their mobile devices, they should communicate this to the Board immediately so their email account can be disassociated with their device.

e) Employee Training

The Company's employees are periodically trained on cybersecurity risks and the tools they can utilize to keep our information safe. Common employee related cybersecurity issues include improper protection of a Company computer or mobile device, poor password management, not utilizing two-factor authentication, the inability to recognize email phishing attacks or using outdated anti-virus software. Employees are made aware of the cybersecurity threats made towards our organization and are taught to be vigilant.

Malicious actors may try to pose as Company's customers and attempt to wire proceeds to their accounts. To avoid this from happening, employees will verbally confirm all wire requests with the phone number (Call back) we have on file for such customers.

In the event of a cybersecurity event, the Board members will notify all employees and instruct them to change all passwords. The Board will notify all investors/clients of the nature of the event and how we are working to remediate the situation. The Company will work with its third-party security vendors to resolve the security issue.

f) Incident Response

In the event of a cybersecurity issue, the Company's Board will take immediate actions with the support of the IT teams/support to rectify the situation. If related to an employee's/officer's email, the e-mail account will be deactivated, and the Company will follow the procedures created to notify all parties involved. The Company with the support of the IT team will scan the network for any data loss, email hacking and will notify all employees to scan their anti-virus software. If any vendors or clients are involved, the Company will alert them as soon as possible and instruct them to delete any suspicious emails.

The Company will document all incidents and their remediation efforts. Company employees have enabled two-factor authentication on their email accounts to reduce the likelihood of such attempts.

14. Financial Resources

Relevant officers should ensure that the Company always maintains adequate financial resources to meet its financial obligations and is able to withstand the risks to which the Company is subject to. In light of the above, the Company can observe the following:

- Conducting a solvency test as required under Section 6 of the Mauritius Companies Act 2001 (the "**Companies Act**") prior to distributing funds to its shareholders;
- A letter of support can be requested from the Shareholders to ensure that the financial obligations of the Company can be met;
- To ensure that audited financial statements of the Company are prepared and submitted to the FSC within the requisite deadlines.

a) Protection of Customer's/Company's Assets

Where an officer has control of or is otherwise responsible for assets belonging to the Company which the Company is required to safeguard, he should arrange proper protection for them, by way of segregation and identification of those assets. Officers must not engage in fraudulent or any other dishonest activity involving the property or assets of the Company.

All of the Company's property and assets must not be considered as the officer's personal property. They should only be used for the benefit of the Company. An officer must act with utmost care and diligence to ensure that the Company's customers' funds are not commingled with the Company's own funds or those of its affiliates or funds belonging to other customers. The Company generates, receives and stores information from various sources. Officers have the responsibility to ensure that such information to which they have access or under their control are properly safeguarded. Officers must not make any false and/or artificial entries in the books and records of the Company for any reason.

Officers should not disclose the Company's customers' confidential information or allow such disclosure, unless prior authorization has been obtained from the relevant customers. This obligation continues beyond the termination of the officer's employment with the Company. Officers must use their best efforts to avoid unintentional disclosure of confidential information by adhering to existing processes within the Company and applying special care when storing or transmitting confidential information.

15. Fit and Proper Standards for the Company

a) Competence and Capability

To assess the competence and capability of its officers, the Company will ensure that they act in a knowledgeable, professional and efficient manner by complying with the requirements of the applicable laws. The Company will appoint officers who have:

- appropriate range of skills and experience;
- technical knowledge and ability to perform the prescribed duties for which they will be engaged, especially with recognized professional qualifications and membership of relevant professional institutions;
- relevant satisfactory past performance or expertise.

b) Honesty, integrity and fairness

In determining the honesty, integrity and reputation of the person which the Company intends to engage, the Company will consider whether the person has been convicted of offences such as fraud, dishonesty, money laundering, terrorist financing, theft, or other financial crimes.

c) Financial soundness or Insolvency

The Company will ensure the financial soundness of the Company by imposing adequate control over financial risks on a continuing basis.

16. Anti-Money Laundering, Countering Financing of Terrorism & Proliferation, Anti-Bribery Policy

The Board of the Company (the "**Board**") will implement internal controls and procedures to combat money laundering, financing of terrorism, proliferation and financial crimes as per the requirements of the Financial Intelligence and Anti-Money Laundering Act 2002 ("**FIAMLA**"), the Financial Intelligence and Anti-Money Laundering Regulations 2018 ("**FIAMLR18**"), the Financial Intelligence and Anti-Money Laundering Regulations 2019 ("**FIAMLR19**"), the Anti-Money Laundering And Combatting The Financing Of Terrorism And Proliferation (Miscellaneous Provisions) Act 2024 ("AMLA"), the Financial Crimes Commission Act 2023 ("FCC"), United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 ("UNSA"), the Prevention of Corruption Act 2002 ("POCA"), the Prevention of Terrorism Act 2002 ("POTA"), the FSC Handbook and other relevant guidelines/circulars issued by the FSC.

The Board will put the following into operation:

a) programs for assessing risk relating to the combat against money laundering, financing of terrorism, proliferation, and financial crimes;
b) the formulation of a control policy that will cover issues of timing, degree of control, areas to be controlled, responsibilities and follow-up;
c) monitoring programs in relation to complex, unusual or large transactions;
d) enhanced due diligence procedures with respect to persons and business relations and transactions carrying high risk, and high-risk countries in accordance with section 17H of the FIAMLA, and with persons established in jurisdictions that do not have adequate systems in place against money laundering and financing of terrorism;
e) providing employees/officers, with training in the recognition and handling of suspicious transactions among others, from time to time;
f) making employees aware of the procedures under the above mentioned legislations, policies, and guidelines/circulars; and
g) establishing and maintaining a set of Policies/procedures/Framework in relation to the combat against money laundering, financing of terrorism, proliferation, and financial crimes.

i. Control Systems

To assist in the proper monitoring and control of suspicious transactions, the Board should set up a control system by appointing a money laundering reporting officer and a deputy money laundering reporting officer who shall have direct access to the Board. The latter will report to the Board annually via a report or earlier depending on urgency of the matter at hand.

ii. Transaction Examination

Reasonable steps shall be taken to allow the identification of suspicious transactions. In the recognition of suspicious transactions, employees/officers should be particularly aware of the following essential elements among others:

- the usual nature of the client's business;
- the patterns of transactions;
- Red Flags;
- Transaction attempts.

Employees/officers should report all transactions that they **suspect** to be linked to criminal activity via the Company's template internal suspicious transaction reporting form. The following are potential red flags that officers/employees shall pay attention to, among others:

iii. Red Flags:

Red flags that signal possible money laundering or terrorist financing include, but are not limited to:

- The customer exhibits unusual concern about the Company's compliance with government reporting requirements and the Company's AML policies (particularly concerning his or her identity, type of business and assets), or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspicious identification or business documents;
- The customer wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer's stated business or investment strategy;

- The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect;
- Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets;
- The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations;
- The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs;
- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity;
- The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry;
- The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash, or asks for exemptions from the Company's policies relating to the deposit of cash;
- For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers;
- The customer is from, or has accounts in, a country identified as a non-cooperative country or territory by the FATF;
- The customer's account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity;
- The customer's account shows numerous currency or cashier’s check transactions aggregating to significant sums;
- The customer's account has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose;
- The customer's account has wire transfers that have no apparent business purpose to or from a country identified as a money laundering risk or a bank secrecy haven;
- The customer's account indicates large or frequent wire transfers, immediately withdrawn by check or debit card without any apparent business purpose;
- The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another Company, without any apparent business purpose;
- The customer makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer of the proceeds out of the account;
- The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose;
- The customer requests that a transaction be processed to avoid the Company's normal documentation requirements;
- The customer, for no apparent reason or in conjunction with other red flags, engages in transactions involving certain types of securities, such as penny stocks, Regulation S stocks, and bearer bonds, which although legitimate, have been used in connection with fraudulent schemes and money laundering activity (Such transactions may warrant further due diligence to ensure the legitimacy of the customer's activity.);
- The customer's account shows an unexplained high level of account activity with very low levels of securities transactions;
- The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, for no apparent purpose; or
- The customer's account has inflows of funds or other assets well beyond the known income or resources of the customer.

17. Procedures to prevent financial crimes

Facilitation payments are defined as “any facilitating payment or expediting payment to a foreign official, political party, or party official the purpose of which is to expedite or to secure the performance of a routine governmental action.” These payments are illegal and are against the Company’s policies. No Covered Person may willingly offer to make, or make, a facilitation payment. If you are asked to make a payment on our behalf, you should always be mindful of what the payment is for and whether the amount requested is proportionate to the goods or services provided. Receipt which details the reason for the payment should always requested. If you have any suspicions, concerns or queries regarding a payment, you should raise these with the Compliance Officer.

The Company will not facilitate the evasion of tax by a client, supplier or other third party, including government officials and contractors, by making payments to offshore bank accounts or by other means which have no commercial basis or clearly could be construed by tax authorities to be to facilitate tax evasion by the recipient.

Any Covered Person must not give, offer, promise, provide, or authorize any charitable donation, CSR project, grant, or sponsorship at the request or for the benefit of a public official, or with the intent or purpose of obtaining any improper benefit. All donations, CSR projects, grants, and sponsorships made by or on behalf of the Company must be pre-approved by the Board in writing. In the first instance, all such requests will be forwarded to the Compliance Officer and the MLRO who after review will submit to the Board for approval.

Political donations made on behalf of the Company are strictly prohibited. Covered Persons are also prohibited from making political donations in their personal capacity that could be associated with a potential or active transaction of the Company or the Fund (and must consider before making a political donation whether it is or could be perceived as such). All Covered Persons must disclose to the Compliance Officer and the MLRO all previous personal political donations made in the last 12 months that are associated or could be perceived to have an association to the potential Fund’s opportunity. The MLRO will determine whether additional action is required.

It is often difficult to determine whether a specific circumstance might represent a violation of law. Therefore, it is imperative that all Covered Persons read and understand this Manual and the FCCA and ask questions if any aspect of the Manual or the law is unclear. Covered Persons are encouraged to be aware of “Red Flags” which might suggest that a closer look at the transaction or relationship is necessary before proceeding.

If a Covered Person encounters any Red Flags while working, they must report them promptly to the Compliance Officer and the MLRO. Red Flags might include unusual payments or financial arrangements, such as:

a. Payments to a numbered bank account with no additional details available.
b. Payments to accounts in countries or geographic locations other than where the third party is located, or business is to be performed; or
c. Cash payments.
d. Transactions involving unusually high commissions.
e. Questionable reputation, accusation, or confirmation of engagement in improper business practices of agent or consultant.
f. Refusal by a third party or representative to enter a written contract, or provide a certification, stating it will not take any action that would violate anti-bribery or anti-corruption laws.
g. Lack of transparency as to expenses in accounting records.
h. Inflated invoices, refusal to provide invoices, or overly general statements of services provided in invoices.
i. Third party demands an unexpected additional fee or commission to facilitate a service.
j. Unusually lavish business courtesies, gifts, or entertainment offered or requested.
k. Relationship between the agent/consultant and a government or Public Officials.

l. Apparent lack of qualifications or resources on the part of the third party or representative to perform the services offered.
m. Recommendations for a third party or representative that come from a public official or a potential government customer.

18. Risk Based Approach

a) Aims of adopting a risk-based approach

A risk-based approach towards the prevention and detection of money laundering, terrorism financing, proliferation and financial crime aims to support the development of preventative and mitigating measures that are commensurate with the money laundering, terrorism financing, proliferation and financial crime risks identified by the financial institution. This approach also aims to deal with those risks in the most cost-effective and proportionate way.

Section 17 of the FIAMLA provides for a duty for the financial institution to identify, assess and understand its money laundering and terrorism financing risks. Furthermore, section 17 (A) of the FIAMLA requires a financial institution to establish policies, controls and procedures to mitigate and manage effectively the risks of money laundering and terrorism financing identified in any risk assessment undertaken by the financial institution. In this respect the Company shall ensure that the Board/officers/employees understand the money laundering, terrorism financing, proliferation and financial crime risks and the Company shall ensure that it has in place effective policies, procedures, and controls to identify, assess, understand, mitigate, manage, and review and monitor, those risks in a way that is consistent with the requirements of section 17 of the FIAMLA, the AMLA, the FCC Act, and the requirements of the FSC Handbook.

A risk-based approach starts with the identification and assessment of the risk that has to be managed. A risk-based approach requires the financial institution to assess the risks of how it might be involved in money laundering, terrorism financing, proliferation and financial crime, taking into account its customers (and the beneficial owners of customers), countries and geographic areas, the products, services and transactions it offers or undertakes, and the delivery channels by which it provides those products, services and/or transactions.

The Company shall conduct a risk appetite review annually and set out the results in a risk appetite statement signed by a Director. In parallel, the Company shall conduct its enterprise-wide risk assessment annually and table same for Board approval.

It should be noted, however, that a risk-based approach does not exempt the Company from the requirement to apply enhanced measures where it has identified higher risk factors, as detailed in the FSC Handbook.

b) Business Risk Assessment

The BRA is the first part of the enterprise-wide risk assessment while the second part is the customer risk assessment and any other related third-party risk assessments as applicable. The BRA involves making a judgement of a number of elements including threat, vulnerability and consequence. It should also consider the extent of its exposure to risk by reference to a number of additional factors. A key component of a risk-based approach involves the Company identifying areas where its products and services could be exposed to the risks and taking appropriate steps to ensure that any identified risks are managed and mitigated through the establishment of appropriate and effective policies, procedures and controls. The BRA shall be reviewed annually, shall be of good quality and serve as a vital contribution to determine the Company’s policies, procedures and controls are proportionate and targeted appropriately.

BRA, and supporting analysis undertaken during the exercise shall be kept on record. The BRA Report shall indicate the mitigative measures undertaken against risks identified.

Section 17(2) of the FIAMLA requires businesses to assess 6 key areas when undertaking the BRA amongst other risk factors:

1. The nature, scale and complexity of the financial institution's activities;
2. The products and services provided by the financial institution's;
3. The persons to whom and the manner in which the products and services are provided;
4. The nature, scale, complexity and location of the customer's activities;
5. Reliance on third parties for elements of the customer due diligence process; and
6. Technological developments.

As per Section 17(2) (b) of the FIAMLA, financial institutions shall take into account the findings of the National Risk Assessment ('**NRA**') and any guidance issued in their BRA.

For completeness, the assessment should consider the operational risks, reputational risks and legal risks posed by the use of new technologies in the context of money laundering, terrorism financing, proliferation and financial crime. Appropriate action should be taken to mitigate the risks that have been identified.

c) Customer Risk Assessments

A CRA estimating the risk of money laundering, terrorism financing, proliferation and financial crime is undertaken prior to the establishment of a business relationship or carrying out an occasional transaction, with or for, that customer. This risk assessment is documented in order to be able to demonstrate its basis and is a living document that is revisited and reviewed, as and when more information about the customer and relationship is obtained. The CRA will be conducted for each client at onboarding and thereafter reviewed in the form of risk buckets as per latitude extended by the FSC Handbook .

The initial risk assessment of a particular customer will help determine, at a minimum:

- The extent of identification information to be sought;
- Any additional information that needs to be requested;
- How that information will be verified; and
- The extent to which the relationship will be monitored on an ongoing basis.

Due care shall be exercised under a risk-based approach. Being identified as carrying a higher risk does not automatically mean that a customer is a money launderer or is financing terrorism. Similarly, identifying a customer as carrying a lower risk does not mean that the customer presents no risk at all. Upon completion of the risk assessment any additional information, evidence or clarification is sought in the event that circumstances remain unclear.

d) Omnibus Accounts

Omnibus account relationship may be established with an applicant for business which is a regulated financial institution based either in Mauritius or in an equivalent jurisdiction. CDD measures should be undertaken on the applicant for business itself. And in addition to identifying and verifying the applicant for business, the following should be complied with:

(i) Gather sufficient information regarding the applicant for business (the financial institution) to understand its business and to determine from publicly available information its professional reputation;
(ii) Assess the adequacy of the financial institution's CDD process;
(iii) Obtain the AML, CFT and Sanctions framework and policy of the financial institution;
(iv) Obtain an AML, CFT and sanctions undertaking letter from the financial institution/bank;
(v) The financial institution is required to complete the AML Questionnaire to the satisfaction of the Company;
(vi) Ascertain whether the financial institution has a physical presence in the jurisdiction in which it is incorporated. The Company shall not establish nor maintain an omnibus account for a financial institution that has neither a physical presence in that jurisdiction nor is affiliated with a regulated financial group that has such a presence;
(vii) Where the financial institution is a foreign entity, ensure that the country in which it is located is an equivalent jurisdiction with a view to determine whether the Client has been subject to sufficient CDD standards. Where the financial institution is located in a non-equivalent jurisdiction, the prior approval of the FSC must be sought before accepting such Clients;
(viii) Obtain board's approval before establishing a new omnibus account relationship; and
(ix) Document the respective responsibilities of each institution.

19. Suspicious Transactions and Reporting

a) Monitoring Accounts for Suspicious Activity

The Company shall monitor account activity to permit identification of patterns of unusual size, volume, pattern or type of transactions, geographic factors such as whether jurisdictions designated as "non-cooperative" are involved, or any of the "red flags" identified above found. Monitoring shall be conducted by the dealing team, the payment processing team, the customer onboarding team, the complaints handling team, among others. The Compliance Team will also conduct monitoring on a sample basis and report back the outcome in the Compliance Report. Similar approach will be undertaken by the MLRO (or DMLRO) regarding sample checks and reporting via a MLRO Report. Evidence of analysis shall be maintained on record.

The Company shall pay attention to all transactions, including trading activities, deposits from customers, inward remittances in company accounts (bank/electronic money institutions/ payment service provider accounts), inclusive of client accounts and corporate accounts, payment transfers, among others, to determine if a transaction is legitimate or lacks financial sense or is suspicious.

Based on such monitoring, the officer shall determine whether to file an internal suspicious transaction report or an exception report to the MLRO (or in his/her absence, the DMLRO) that include transaction size, transaction type, location, details, number, and nature of the activity. Employee guidelines with examples of suspicious activity are enclosed to the policy where client profiles may warrant further scrutiny.

After receipt of the suspicious transaction report, the MLRO, shall investigate the case and, if deemed suspicious, shall make a report to the FIU via the GoAML platform.

b) Emergency notification to the regulators by telephone regarding sanctions

When conducting due diligence or opening of an account, the Company shall immediately connect with law enforcement organisations in these emergency scenarios:

- Discovery of listed party in a structure;
- Discovery of an account holder or party located in a country or region listed on the OFAC list,
- Discovery of an accountholder which is held by an entity that is owned or controlled by a person or entity listed on the OFAC list,
- a customer tries to use bribery, coercion, or similar means to open an account or carry out a suspicious activity,
- we have reason to believe the customer is trying to move illicit cash out of the government's reach
- we have reason to believe the customer is about to use the funds to further an act of terrorism.

c) Responding to Red Flags and Suspicious Activity

When a member/officer of the Company detects any red flag(s) he or she will investigate further under the guidance of the CO. This may include gathering additional information internally or from third-party sources.

Where a suspicion exists on any transaction, the member/officer must immediately report the matter to the MLRO (or in his/her absence to the DMLRO). It is vital not to inform any other person involved in the transaction or any unauthorised third party that this transaction has been reported to the MLRO as this may amount to an offence under the FIAMLA.

Note: Section 12 (6) of the FIAMLA indicates that "…The Board shall not have the power to consider, discuss or deliberate on any matter relating to the lodging, analyzing, reporting, requesting or disseminating of information in respect of any suspicious transaction report, nor will it have access to information concerning any suspicious transaction report…"

The MLRO and DMLRO shall ensure that they are registered on the GoAML platform at all times and ensure that an internal and external STR log is maintained at all times.

20. Business Continuity Plan ('BCP')

a) Background

While it is recognized that it is not possible to create a plan to handle every possible event, it is the intent of this Company to set up a framework to be used in most likely of scenarios. It is also the intent that this framework provides guidance as to how to respond should an unforeseen situation occur.

b) Business Description

The Company was incorporated in Mauritius on 1st of September 2025 and holds a Global Business License Company under the Financial Services Act 2007 ("**FSA**") and is authorized to operate as an Investment Dealer under the Securities Act 2005.

c) Company Policy

The Company's policy is to respond to a Significant Business Disruption (SBD) by safeguarding employees' lives and Company property, making a financial and operational assessment, quickly recovering and resuming operations, protecting all of the Company's books and records, and allowing our clients to transact business. In the event that we determine we are unable to continue our business, we will assure clients prompt access to their funds and securities.

d) Significant Business Disruptions ('SBD')

Our plan anticipates two kinds of SBDs, internal and external. Internal SBDs affect only our Company's ability to communicate and do business, such as a fire in our building or the death of a key member of the Company. External SBDs prevent the operation of the securities markets or a number of firms, such as a terrorist attack, a city flood, or a wide-scale, regional disruption including epidemics, pandemics and outbreaks. Our response to an external SBD relies more heavily on other organizations and systems, such as the custodian we use.

In the event of an internal SBD such as a fire or flood in one of our offices, employees are instructed to work remotely until the building is safe for use again. An internal SBD such as a death of a key member of the Company will not warrant employees to work remotely and the manager in charge will follow the guidelines issued by Board.

In the event of an external SBD, if local or central governments deem it necessary to stay home from work and avoid public places, all employees are instructed to work remotely. Employees should be available by e-mail and telephone if possible.

e) Approval and Execution Authority

The Board, is responsible for approving the plan and for conducting the required annual review. The Board has the authority to execute this BCP.

f) Plan Location and Access

The Company will maintain copies of the BCP and annual reviews, and all changes that have been made to it. A physical copy of the BCP will be stored with the Company's written policies and procedures manual.

g) Alternative Physical Location(s) of Employees

In the event of an SBD that makes it impossible or impractical to use the Company offices, all employees are instructed to work remotely at their homes or in another safe location. Employees should avoid using public Wi-Fi.

h) Data Back-Up and Recovery (Hard Copy and Electronic)

The Company maintains its primary hard copy books and records and its electronic records at its registered office. The Company maintains the following document types and forms: Policy Statements, Client Contracts, due diligence documents, service provider contracts and other related documents.

The Company keeps all of its data stored electronically on a cloud-based system which is backed up instantaneously.

i) Operational Assessments

- Operational Risk

In the event of an SBD, we will immediately identify what means will permit us to communicate with our clients, employees, critical business constituents, and regulators. Although the effects of an SBD will determine the means of alternative communication, the communications options we will employ will include our website, telephone voice mail, secure e-mail, etc.

- Mission Critical Systems

Our Company's "mission critical systems" are those that ensure client communication, access to client accounts and trading systems. More specifically, these systems include the office computer systems.

We have primary responsibility for establishing and maintaining our business relationships with our clients. Our custodian provides the execution, comparison, allocation, clearance and settlement of securities transactions, the maintenance of customer accounts, access to customer accounts, and the delivery of funds and securities.

Our custodian contract provides that our brokerage firm will maintain a business continuity plan and the capacity to execute that plan.

Our custodian represents that it backs up our records at a remote site. Our custodian represents that it operates a back-up operating facility in a geographically separate area with the capability to conduct the same volume of business as its primary site. Our custodian has also confirmed the effectiveness of its back-up arrangements to recover from a wide scale disruption by testing.

j) Our Company's Mission Critical Systems

- Trading

Currently, our Company enters trades by recording them on paper and electronically and sending them to our brokerage firm electronically or telephonically.

In the event of an internal SBD, we will enter and send records to our brokerage firm by the fastest alternative means available. In the event of an external SBD, we will maintain the order in electronic or paper format and

deliver the order to the brokerage firm by the fastest means available when it resumes operations. In addition, during an internal SBD, we may need to refer our clients to deal directly with our brokerage firm for order entry.

- Client Account Information

We currently access client account information via the custodian. In the event of an internal SBD, we would access client information via fax correspondence, alternate phone systems, etc.

k) Alternate Communications with Clients, Employees, and Regulators

- Clients

We now communicate with our clients using the telephone, e-mail, our website, fax, and mail. In the event of an SBD, we will assess which means of communication are still available to us, and use the means closest in speed and form (written or oral) to the means that we have used in the past to communicate with the other party. For example, if we have communicated with a party by e-mail but the Internet is unavailable, we will call them on the telephone and follow up where a record is needed with paper copy in the mail.

- Employees

We now communicate with our employees using the telephone, e-mail, and in person. In the event of an SBD, we will assess which means of communication are still available to us, and use the means closest in speed and form (written or oral) to the means that we have used in the past to communicate with the other party.

- Regulators

We communicate with our regulators using the telephone, e-mail, fax, mail, and in person. In the event of an SBD, we will assess which means of communication are still available to us, and use the means closest in speed and form (written or oral) to the means that we have used in the past to communicate with the other party.

l) Regulatory Reporting

Our Company is subject to regulation by the Mauritius FSC. We file reports with our regulators using paper copies in the mail, and electronically using fax, e-mail, and the Internet. In the event of an SBD, we will check with the relevant regulators to determine which means of filing are still available to us, and use the means closest in speed and form (written or oral) to our previous filing method.

In the event that we cannot contact our regulators, we will continue to file required reports using the communication means available to us.

Regulatory Contact
The Chief Executive
Financial Services Commission
54 Ebene Cybercity
Ebene, Mauritius, 230-403-7000

m) Orderly Unwinding Procedures

In the event that the entire Company is incapacitated, the administrator will work in consultation with the Board Members to ensure orderly unwinding of the portfolio. The administrator will sell 10% of the portfolio every other business day, utilizing different brokers. Once the entire portfolio has been liquidated, the administrator will trigger voluntary distributions and will disperse the proceeds to each limited partner.

The administrator will be responsible for handling payments to any creditors or vendors.

n) Updates and Annual Review

Our Company will update this plan whenever we have a material change to our operations, structure, business or location or to those of our brokerage firm. In addition, our Company will review this BCP annually, to modify it for any changes in our operations, structure, business, or location or those of our brokerage firm.