May 2022

License no. GB21026947

MEGA FINANCE

Policies and Procedures Manual

Version 1.0

Policy Statement

It is unlawful for a Registered Investment Dealer (**"RID"**) to provide investment advice unless the RID has adopted and implemented written policies and procedures reasonably designed to prevent violation of regulations and rules by the RID or any of its supervised persons. The rule requires dealers to consider their fiduciary and regulatory obligations under the Mauritius Financial Services Commission ("**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.

Compliance Officer 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, Lindholm Capital Ltd (the "**Company**"). The Compliance Officer ("**CO**") has a position of sufficient seniority and authority within the organization to compel others to adhere to the compliance policies and procedures.

Compliance Officer	Date Responsibility Assumed
Mr. Kishen Hurhinidee	20 JANUARY 2022

Fiduciary Statement

Background

The Company holds a Global Business License ("**GBL**") issued by the FSC on 20 January 2022, as well as, an Investment Dealer Full-Service Dealer, excluding Underwriting license (the "**ID License**"), granted by the FSC on 20 January 2022.

An investment dealer 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 investor would consider them to be important. 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.

Company Statement

MEGA FINANCE is an Investment Dealer (Full-Service Dealer, excluding Underwriting), regulated by the **Financial Services Commission ('FSC') in Mauritius** under the license number **GB21026947** (hereinafter referred to as "**MGF**" or the "**Company**").

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.

Code of Ethics Statement

Background

In accordance with regulations, the Company has adopted a code of ethics to:

- Set forth standards of conduct expected of advisory personnel (including compliance with securities laws);
- Safeguard material non-public information about client transactions; and
- Require "access persons" to report their personal securities transactions.

Introduction

As a holder of the ID License, 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, 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 all of their relevant staff, obtain registration (where applicable) under relevant regulations.

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 misleading advertisements or intrude upon the privacy
of
the public through door-to-door canvassing or other similar methods.

12. The Company and all its group entities shall provide investors with all requisite documentation promptly in accordance with their stated intentions.

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 will be binding on all officers, advisers, managers 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 officer, adviser, manager 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 employment.

Prohibited Purchases and Sales

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 who are aware of the misuse of material non-public information should report such to the CO. This policy applies to all of the Company's employees and associated persons without exception.

The CO collects and maintains a list of each access person's personal securities owned. The CO reviews the summaries for inappropriate transactions and report them to the CO for action. Access persons report their personal securities' transactions on at least a quarterly basis and annually thereafter.

Prohibited Activities

Conflicts of Interest Policy

MEGA FINANCE is an Investment Dealer (Full-Service Dealer, excluding Underwriting), regulated by the **Financial Services Commission ('FSC') in Mauritius** under the license number **GB21026947** (hereinafter referred to as "**MGF**" or the "**Company**").

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."

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 Code of Ethics:

- 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

[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.

or its affiliates, to the Compliance Officer ('CO'). If the CO 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 its 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 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.

The Company and its officers will act in the best interest of its clients.

- An interests register will be kept by the Company.
- 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.

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 Advisory Functions;

- Independent oversight;
- Disclosure;
- Declining to provide the service.

A conflict-of-interest register shall be kept by each Committee. Any conflict-of-interest situation or potential conflicts' situation should be reported immediately to the relevant Committee who shall escalate it to the Board of the Company.

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 CO. 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 the CO 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.

Political and Charitable Contributions

Supervised persons that make political and charitable contributions, in cash or services, must report each such contribution to the CO, who will compile and report thereon as required under relevant regulations. Supervised persons are prohibited from considering the ID's current or anticipated business relationships as a factor in soliciting political or charitable donations. This policy is only enforced if a government entity is a client of the Company.

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.

Service on Board of Directors

Supervised persons shall not serve on the board of directors of publicly traded companies absent prior authorization by the CO. 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.

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.

Compliance Procedures

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.

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 CO 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 CO / 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 CO on the written authorization response.
4. Records of all pre-clearance requests and responses will be maintained by the CO for monitoring purposes and ensuring the Code of Ethics is followed.

B. Pre-Clearance Exemptions

The pre-clearance requirements of this section of this Code of Ethics 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.
10. Employees in the U.S. office are exempt from pre-clearance rules given the zero overlap in securities investments of the Company and time zone constraints.

C. Reporting Requirements

1. Holdings Reports

Every access person shall, no later than ten (10) days after the person becomes an access person and annually thereafter, file a holdings' report containing the following information:

a. The title and number of shares of each Reportable Security in which the access person had any direct or indirect beneficial ownership when the person becomes an access person;
b. The name of any broker, dealer or bank with whom the access person maintained an account in which any securities were held for the direct or indirect benefit of the access person; and
c. The date that the report is submitted by the access person.

2. Transaction Reports

Every access person shall, no later than ten (10) days after a security transaction is executed, file transaction reports containing the following information:

a. For each transaction involving a Reportable Security in which the access person had, or as a result of the transaction acquired, any direct or indirect beneficial ownership, the access person must provide the date of the transaction, the title and number of shares of each involved in the transaction;
b. The nature of the transaction (e.g., purchase, sale)
c. The price of the security at which the transaction was effected;
d. The name of any broker, dealer or bank with or through the transaction was effected; and
e. The date that the report is submitted by the access person.

3. Reporting Exemptions

The reporting requirements of this section of this Code of Ethics shall not apply to:

a. Any report with respect to securities over which the access person has no direct or indirect influence or control.
b. Transaction reports with respect to transactions effected pursuant to an automatic investment plan, including dividend reinvestment plans.
c. Transaction reports if the report would contain duplicate information contained in broker trade confirmations or account statements that the Company holds in its records so long as the Company receives the confirmations or statements no later than thirty (30) days after the end of the applicable calendar quarter.
d. Any transaction or holding report if the Company has only one access person, so long as the Company maintains records of the information otherwise required to be reported under the rule.

4. Report Confidentiality

   All holdings and transaction reports will be held strictly confidential, except to the extent necessary to implement and enforce the provisions of the code or to comply with requests for information from government agencies.

5. Compliance Officer Review of Personal Securities' Information

   The CO or designated compliance officer will review all access person's personal securities transactions and holdings report after they have been collected. The officer will look to identify improper trades or trading patterns by access persons. All violations will be reported to the CO.

Restricted Securities

The Company does not maintain a list of restricted securities that supervised persons are restricted from trading in. The Company requires all personal trades by members of the investment team to be precleared before executing. The Company also requires a "portfolio first" rule. Any security that is being held, sold, or bought in the Company's portfolios, must be executed prior to any of the Company's employee transaction.

Investing Personal Money in the Same Securities as Clients

From time to time, representatives of the Company may buy or sell securities for themselves that is also in our fund and SMAs. The CO will always document any transactions that could be construed as conflicts of interest and the Company will always transact client business before their own when similar securities are being bought or sold.

Certification of Compliance

Initial Certification

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

Acknowledgement of Amendments

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

Annual Certification

All supervised persons must annually certify that they have read, understood, and complied with the Policies and Procedures and that the supervised person has made all of the reports required by this code and has not engaged in any prohibited conduct.

The CO shall maintain records of these certifications of compliance.

Compliance Officer Duties

Training and Education

CO shall be responsible for training and educating supervised persons regarding this Code. Training will occur periodically as needed. All supervised persons are required to attend training sessions, read any applicable materials and acknowledge their training on the attestation provided in the Policies and Procedures manual.

Annual Review

CO shall review and test at least annually the adequacy of the Policies and Procedures and the effectiveness of its implementation. CO will attest that it has been reviewed and updated.

Email Review

CO will randomly review access person's emails once a quarter and document his/her review.

Recordkeeping

CO shall ensure that the Company maintains the following records in a readily accessible place:

- A copy of each code of ethics that has been in effect at any time during the past seven years;
- A record of any violation of the code 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 code 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 code, 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.

The Company must further keep record of:

- the identity and address of the investor;
- 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:
- 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 reports made to and by the MLRO/Deputy MLRO;
  - All training provided in relation to AML and CFT.

Transactional records and or documents are kept at the Company's Administrator's registered office. Records should be sufficient to provide adequate evidence to the relevant local authorities to conduct their investigations.

Client instructions/ on boarding described

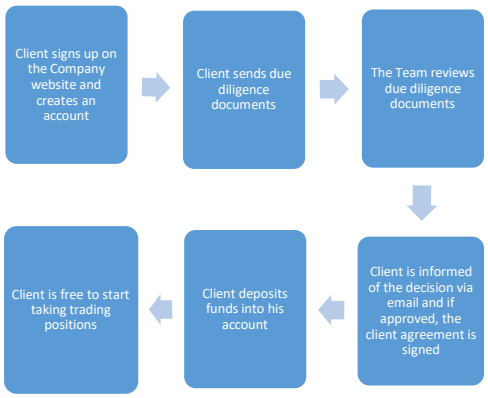
Process:

i. Client initiates contact
ii. Client completes on boarding form online or manually and emails to the Team along with required due diligence documents. The due diligence shall be:
    1. Certified passport copy
    2. Certified proof of address in form of utility bill
    3. Bank details and Source of Funds
iii. The Team conducts a compliance review, pre-screening for completeness of application and also World check screening to check the clients' background. The board of directors will be responsible to approve/reject any client is deemed to be high risk;
iv. The Team communicates the decision to the client
v. If approved the client's online account is activated and client informed to fund the account.

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



Advertising Policy

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

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.

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.

Accuracy of Disclosures Made to Investors, Clients, and Regulators

The CO is responsible for the accuracy of all disclosures made to clients, and regulators. Where third party disclosure documents are involved, the CO will verify that these documents are legitimate documents from the third party. The Company will notify all clients receiving these third-party documents that the Company has only verified the legitimacy and origin of the documents but has NOT verified or analyzed the information contained therein. The client will be instructed to conduct their own investigations to verify the information contained in each document including but not limited to a due diligence investigation.

Account Statements

The Company will review client account statements to ensure their accuracy. All client account statements will be stored electronically. Investors should refer to their custodial statements for an official record.

Advertisements

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

Privacy Policy

The privacy policy statement is given to clients at the initial signing of the client contract and emailed once annually. A copy of the privacy policy is available on our website and can be provided at request.

Trading Policies

1. Introduction

MEGA FINANCE is an Investment Dealer (Full-Service Dealer, excluding Underwriting), regulated by the **Financial Services Commission ('FSC') in Mauritius** under the license number **GB21026947** (hereinafter referred to as "**MGF**" or the "**Company**").

2. Best Execution Obligation

The Company owes a fiduciary duty to clients to obtain best execution of their brokerage transactions. Failure by the Company to fulfill its duty to clients to obtain best execution may have significant regulatory consequences. The Company's policies are modeled after the guidelines articulated by the regulators; specifically, it believes that, to a significant degree, best execution is a qualitative concept. In deciding what constitutes best execution, the determinative factor is not the lowest possible commission cost, but whether the transaction represents the best *qualitative* execution. In making this determination, the Company's policy is to consider the full range of the broker's services, including without limitation the value of research provided, execution capabilities, commission rate, financial responsibility, administrative resources and responsiveness.

Execution by brokers: All trades are electronic, fully regulated and transparent.

2.1.Trading Process

2.1.1. Opening a Position (CFDs)

Steps:

i. Client logs into own online account and issues instruction to open a trading position clicking preferred CFD product and intended trade move (buy/sell)
ii. The Team receives electronic instruction
iii. Initially, the Team reviews the order for compliance with the law and exchange trading rules
iv. Order sent to dealing department for execution
v. Dealing Department immediately sends the trade instruction to the liquidity provider (Diagram 2)/ Dealing Department executes the trade in cases of dealing on own account (Diagram 3)
vi. Confirmation is sent to the client account confirming trade has been placed/executed and account position updated on the platform

Diagram 2: Diagram showing Order Execution Flow Chart when the Company acts as an intermediary to the transaction.

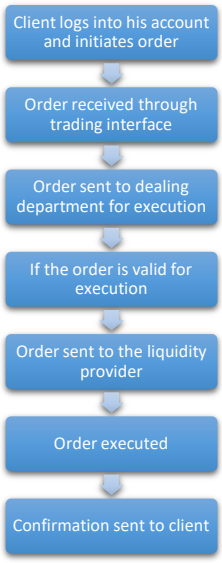
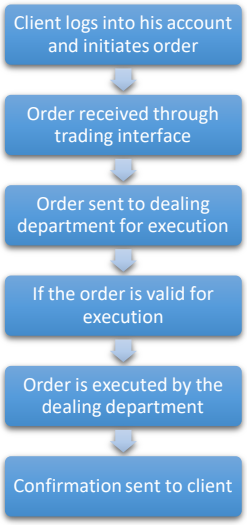


Diagram 3: Diagram showing Order Execution Flow Chart when the Company is dealing on own account



2.1.2. Closing a Position (CFDs)

Steps

i. Client logs into own online account and issues instruction to open a trading position clicking preferred CFD product and intended trade move (buy/sell)
ii. Client issues instruction to close a trading position by clicking the target open CFD contract and instructs to close out position
iii. The Team receives electronic instruction and reviews for compliance with trading rules
iv. The instruction to close the trading position is automatically sent to the liquidity provider/ Dealing Department reviews, approves and closes the trade when dealing on own account
v. Confirmation is sent to the client account confirming trade has been placed/executed and account position updated

2.1.3. Withdrawal Process

i. Client logs into online account or send us an email and instructs us of his decision to withdraw
ii. The Team evaluates request vis a vis open trade positions and margin call requirements along with exchange trading rules.
iii. The Team submits withdrawal instruction along with destination bank account details to compliance for approval
iv. The Team approves/rejects request
v. If approved finance issues payment via wire or any other permitted mode of payment.
vi. The Team communicates to client of confirmation of wire via email and online account

2.1.4. Trades Confirmations

Once the trade has been executed, the client will see on his/her account, and at the end of each day, the Company sends a statement with the following:

a. Closed Transactions
b. Open Trades
c. Working Orders
d. Financial position

2.2.Execution of trades

How we shall ensure best execution of client trades. All trades are executed to leading liquidity banks using market execution with no re-quotes, no dealing desk or human intervention and no trading restrictions.

The Company will ensure the feeds provided are for best execution of its clients through provision of Best Execution, the Company takes into account the following Execution Factors:

- price;
- costs payable by the client as a result of execution;
- speed of execution;
- likelihood of execution;
- size and nature of the order;
- likely market impact;
- risks relevant to the execution;
- nature of the market for the Financial Instrument, and;
- any other consideration deemed relevant to the execution of the order.

3. Execution Venues

This Best Execution Policy sets out the venues on which we may transact your order. We will act as the sole execution venue for all client orders which are executed on an 'Over the Counter' (OTC) basis. We have identified those venues on which we will most regularly seek to execute your orders, as well as venues that we believe offer the best prospects for achieving the best possible results for you, taking into account the factors detailed below.

We are able to transact trades on your behalf via the following execution venues:

i. Our liquidity providers;
ii. Regulated markets;
iii. Where appropriate our customer base in the over the counter (OTC) markets;
iv. Multilateral trading facilities operated by a third party;
v. Systematic internalizers.

When selecting the venue on which to transact trades we will take reasonable measures to ensure that the selected venue obtains the best possible trading result for our clients, subject to the following factors:

i. In the markets in which we operate, we can only give clients visibility to prices that have been communicated to us;
ii. We will provide details of all tradable bids and offers (via the platform and subject to the

other matters referred to below);

iii. Time availability of prices – in many markets there are lulls and spikes in trading as negotiations align trading interests at different times and different parts of the curve, accordingly the "last traded" price may not always be available or act as a reliable indicator of current price;

iv. We cannot allow clients to trade in a market unless we are reasonably satisfied that the client (via an agent or otherwise) is capable of settling the relevant trade; and

v. Fees may vary between clients, based on agreements and levels of activity.

4. Trade Errors

A trade error occurs when there is a deviation from the general trading practices involving transactions and settlements of trades for a client's account. Part of the Company's fiduciary obligation is to identify and correct these errors as soon as discovered. It has been accepted in the industry to recognize the following as trade errors:

1. A *sell* is executed as a *buy*;
2. The over/under allocation of a security i.e., a coma is placed in the wrong place or an additional 0 is added (1,000 turns into 10,000);
3. An incorrect ticket symbol (*C* instead of *S*)
4. Trade takes place in an incorrect account number;
5. A purchase or sale order fails to be executed
6. Limit order is executed at market price;
7. Block trades are allocated inaccurately;
8. Client account does not have the funds to settle the transaction;
9. The purchase or sale of securities is transacted in violation of the client's investment profile or guidelines;
10. The purchase or sale of securities for non-discretionary clients are executed prior to or without receiving client consent, or without proper documented authorization.

The following types of errors will not be deemed to be a trade error as defined by your RIA:

1. An incorrect trade that was caught prior to settlement thereby not having a negative impact on your client;
2. A trade that was improperly documented;
3. The rewriting of tickets that describe or correct improperly executed transactions;
4. Errors that are made by unaffiliated third parties (broker/dealer, custodian, etc.). Although keep in mind, as a fiduciary, you are responsible to review the trades and ensure that third party errors are favorably resolved;

The Company's policy is to ensure that clients are never responsible for a trade error. If the Company is responsible for the error, it will correct the error the same day if possible. If a third party is responsible, the Company will oversee the resolution. Any loss will be reimbursed to the client in the form of a statement credit or check written by the Company, if the custodian or broker/dealer does not cover it under the de minimis.

All trade errors must be timely addressed to the Compliance Officer ('CO') once discovered. The CO should document when the trade error and whether the Company is responsible. If responsible, the Company must then look to correct the error immediately, following fiduciary standards acting in the

client's best interest. Any client losses must be reimbursed by the Company for the full amount of the loss, including the reimbursement of the transaction fees. If there is a profit resulting from the error:

1. The Company may elect to allow the client to retain the profit;
2. The custodian of broker/dealer may retain the profit; or
3. It is best practice to hold the profits in a Company trade error account in accordance with the Company's accounting standards and donated to charity annually.

All payments made to clients will be properly documented.

5. Trade Error File

The Company will maintain a trade error log. All trade errors will be properly documented and maintained by the CO.

6. Market Execution

Market execution is when an order is executed at the best price available directly to the markets, where global banks and financial institutions act as liquidity providers. Orders are executed without any dealing desk manipulation or intervention. Market orders do not experience re-quotes and are executed on a "fill or kill" basis. By using leading broker technologies, traders experience low latency, fast execution and accurate order filling that are beneficial for high frequency traders and scalpers.

7. Use of Technologies to Reduce Latency

Fast order execution is critical to ensure that orders are filled accurately, however, latency can cause delays and lead to orders being filled at the next available price (slippage). The Company tackles latency head on by using fast platform to execute orders with superior, fast and low latency order execution for every trader.

8. Slippage

When trading market execution there are no re-quotes and no orders are rejected, however normal latency in the markets can lead to orders being executed at the next available price (slippage). Slippage is often referred to as negative, but in fact slippage can also be positive for the trader as they experience price improvement with best execution policies.

When exiting an order or when your stop loss/take profit is attempting to be filled, rapid market movements could mean that the price you want to fill at is not available to trade in the market (it past already or didn't exist in the market) and the order is filled at the next available price. Slippage is more likely during volatile market conditions when quoted prices are fluctuating rapidly.

To increase your execution speeds and lower latency, the Company offers a free Virtual Private Server (VPS) Hosting facility that allows clients to trade rapidly and efficiently.

9. Trading Strategies

Pre- and Post-Trade transparency is an important factor for all trading strategies and all clients should assess any Broker conflicts of interests, transparency, conditions and execution philosophies. At the

Company, we support high frequency trading, profitable expert advisors and specialist strategies by offering transparent and beneficial trading rules such as no minimum market distance limits, core spreads and minimum market increments to deliver the best environment we can for you to trade successfully.

10. Monitoring of trade

The Company will put in place a robust trade monitoring system. With our systems and trade compliance monitoring processes, we are able to monitor and detect rogue algorithms in real-time, check for the manipulation of the market at the end of the day and everything in between. Our proven platform and experienced, well-trained employees of the dealer team enable us to combine real-time and historical data to detect suspicious trading patterns on our platform.

Trade monitoring cycle shall be in two phases;

a. Pre-trade monitoring;
b. Post trade monitoring.

A summary of the monitoring processes, mechanisms and capabilities are detailed below.

a. Human Surveillance
    - Real time and post trade monitoring via trade / order surveillance system to detect market abuse and improper trading behaviour
    - Escalating suspicious transactions and conducting follow-up investigations
    - Monitoring of electronic and voice communications to meet regulatory requirements
    - Undertaking ad-hoc monitoring reviews (both desk-based and thematic reviews) in line with the Compliance Monitoring Plan
    - Identifying front office training needs highlighted during monitoring and business reviews
    - Assisting with audit visits and investigations or queries from regulators
    - Assisting with ad hoc work, investigations and projects as required
    - Liaising with all internal control functions to assist in the identification of monitoring-related issues, and the resolution and closing of outstanding monitoring, investigation or other control findings
    - Assisting in the preparation of compliance management information

b. The Company monitors its execution arrangements on an ongoing basis by selecting appropriate samples of orders executed and evaluating the samples as described below:
    - Evaluation of Execution Quality:
        - Price Latency
        - Speed of Execution
        - Frequency and Duration of Price Freezing
        - Depth of Liquidity
        - Price Transparency
        - Re-quotes
    - Comparing prices relayed by price feed providers with the prices quoted by the Company
    - Monitor Slippage on a regular basis to identify whether is asymmetric or not
      Monitor IT infrastructure (responsiveness of interfaces used, adequate integration with data providers, etc.)

c. MT4/MT5 Trade Compliance monitoring capabilities
Assisting the trade monitoring shall be a string trade monitoring module within our MT4/MT5 trading platforms. Below is a summary of the capabilities of the said software.

Capability	Detail
Pre-defined alert scenarios	We have a robust mechanism built to alert the investment dealer team of risk scenarios of various nature, including but not limited to; • Insider trading • Front running • Wash trades • Price ramping • Layering • Quote stuffing • Order-to-trade ratio monitoring • Trading volume spike • Trading price spike • Spreads and comparisons • Passive and large orders monitoring
Alert & case management	The trade monitoring system is organized such that we have a convenient and robust case management module. This includes such capabilities as; • Feature-rich tools to triage alerts and manage investigations • Fully audited workflow
Reporting	• Pre-defined reports to support investigations and manage operational performance

We shall therefore combine human skill, experience and technology to ensure we monitor trading activity diligently to ensure that our traders observe all laws, rules, guidelines and international best practice.

11. Portfolio Management Processes

The Company provides discretionary account management on a continuous basis. The Company invests in public equities, cash and other securities that are deemed suitable, governed by the investment management agreements in place. Certain investors may require pre-approval prior to investing in any securities other than public equities, which is stated in any such side letter.

12. Research Processes

The investment team utilizes information obtained from a wide variety of sources. Increasingly, the Internet and new databases provide a wealth of ideas and information to enhance the Company's research.

Industry research is used to supplement the Company's own research efforts. The Company employees research investments on a daily basis. Examples of on-line resources include financial news websites, and Reuters.

Information Security & Cybersecurity

Th 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 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.

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.

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, VPNs, and using unique passwords on computers, documents and third-party technology systems used.

The Company recognizes that employee's emails are susceptible to potential hacks or malicious phishing attempts. To avoid these events, all employees 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.

Access Control Policy

Company's employees 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.

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 are 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. Employees are instructed to use the Company's VPN, which is mandated while traveling and using public Wi-Fi.

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

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 investors and attempt to wire proceeds to their accounts. To avoid this from happening, employees will verbally confirm all wire requests with the phone number we have on file for such investor.

In the event of a cybersecurity event, the CO will notify all employees and instruct them to change all passwords. The CO will notify all investors 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.

Incident Response

In the event of a cybersecurity issue, the Company's compliance officer will take immediate action to rectify the situation. If related to an employee's email, the e-mail account will be inactivated and follow the procedures created to notify all parties involved. The CO 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 CO will alert them as soon as possible and instruct them to delete any suspicious emails.

The Company has enabled automatic email alerts that are sent to the CO and CEO if Google detects any phishing scams, suspicious logins, or any other cybersecurity incidents. The CO 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.

Financial Resources

Relevant officers should ensure that the Company always maintains adequate financial resources to meet its financial obligations and 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.

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.

Fit and Proper Standards for the Company

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.

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.

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.

Customer Complaint Policy

1. Introduction

This Policy regulates effective, clear and fast handling of complaints and disputes submitted to the Company in relation to the performance and procedures of the Company.

MEGA FINANCE is an Investment Dealer (Full-Service Dealer, excluding Underwriting), regulated by the **Financial Services Commission ('FSC') in Mauritius** under the license number **GB21026947** (hereinafter referred to as "**MGF**" or the "**Company**").

The Company must develop and put into practice an independent and objective complaints resolution system, as provided below.

2. Submitting a Complaint

The complainant, if possible, should report the event or the date of the occasion subject of the complaint to the Company, as soon as possible. This is necessary to enable the Company to investigate the complaint as efficiently as possible. The Company's Compliance Officer shall be responsible for handling complaint reviews. All clients' complaints against the Company shall be directed to XXX.

Commented [EC1]: TO BE COMPLETED

3. Registration of Complaints

The Company shall maintain a complaints' register (the "**Complaints Register**") to record all complaints received. The record shall include the date on which the complaint has been made, date acknowledged, category of complaints and actions taken.

The Company pays special attention to avoid collection of data about the complainant with the exception of recording data aimed to settle the complaint.

Furthermore, the Company manages complaints within a transparent system; complaints shall be traced and administered in each and every stage of the procedure.

4. Managing Complaints

The Company deals with all complaints and all complainants equally, without any discrimination, in harmony with the procedure regulated by this Policy.

All complaints shall be taken seriously, handled transparently and promptly investigated. The Compliance Officer ('CO') shall ensure that all complaints be dealt with in an independent courteous and efficient manner and resolved within thirty (30) days.

No complaint should be left unresolved and the date the complaint is "closed" should be noted on the complaint filing.

5. Response to Complaints

Receipt of complaints shall be acknowledged by the Company and be dealt with, within thirty (30) days.

Some complaints can be resolved more quickly depending on the facts and the nature of the complaint. If the complaint is more complex and takes longer than thirty (30) business days to resolve, we will communicate the reasons for such delay.

6. Monitoring of Complaints

After settling the complaint, the Company shall preserve every document related to complaints for a period of seven (7) years.

The Company shall be entitled to prepare statistics and reports about complaints, which will be aimed to improve the efficiency of administering complaints.

7. Settlement of Disputes

When the complaint is rejected, the complainant may lodge an appeal at the Financial Services Commission (Mauritius). More information can be found on the FSC's website here https://www.fscmauritius.org/en/consumer-protection/complaints-handling.

Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT)

The Board of the Company (the "**Board**") will implement internal controls and procedures to combat money laundering and financing of terrorism as per the requirements of the Financial Intelligence and Anti-Money Laundering Act 2002 ("**FIAMLA**"), the Financial Intelligence and Anti-Money Laundering Regulations 2018 ("**FIAMLR 2018**"), the FSC Handbook and other relevant guidelines/circulars issued by the FSC.

The Board will put the following into operation:

- programs for assessing risk relating to money laundering and financing of terrorism;
- the formulation of a control policy that will cover issues of timing, degree of control, areas to be controlled, responsibilities and follow-up;
- monitoring programs in relation to complex, unusual or large transactions;
- 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;
- providing employees, including the Money Laundering Reporting Officer, from time to time with training in the recognition and handling of suspicious transactions;
- making employees aware of the procedures under the FIAMLA, FIAMLR 2018, the FSC Handbook and any other relevant policies, guidelines/circulars; and
- establishing and maintaining a manual of compliance procedures in relation to anti-money laundering.

The Board should ensure compliance with the requirements of FIAMLA and FIAMLR 2018 and the following should form part of the above internal controls and procedures to be implemented by the Company:

(i) The Board is responsible for managing the Company effectively and is in the best position to understand and evaluate all potential risks to the financial institution, including those of money laundering and financing of terrorism. The Board must therefore take ownership of, and responsibility for, the business risk assessments and ensure that they remain up to date and relevant. On the basis of its business risk assessment, the Board must establish a formal strategy to counter money laundering and financing of terrorism. Where the Company forms part of a group operating outside Mauritius, that strategy may protect both its global reputation and its Mauritius business. The Board must document its systems and controls (including policies and procedures) and clearly apportion responsibilities for countering money laundering and financing of terrorism, and, in particular, responsibilities of the Compliance Officer ("**CO**") and Money Laundering Reporting Officer ("**MLRO**").

(ii) The Company shall establish and maintain an effective policy, for which responsibility shall be taken by the Board, and such policy shall include provision as to the extent and frequency of compliance reviews. The Board should take a risk-based approach when defining its compliance review policy and ensure that those areas deemed to pose the greatest risk to the firm are reviewed more frequently.

(iii) The Board must consider the appropriateness and effectiveness of its compliance arrangements and its policy for the review of compliance at a minimum annually, or whenever material changes to the Company occur. Where, as a result of its review, changes to the compliance arrangements or review policy are required, the Board must ensure that the Company makes those changes in a timely manner.

(iv) The Company is responsible for appointing a CO. In addition to appointing a CO, an independent audit function to test the money laundering and financing of terrorism policies, procedures and controls of the Company should be maintained.

(v) The Board must ensure that the compliance review policy takes into account the size, nature and complexity of the business of the financial institution, including the risks identified in the business risk assessments. The policy must include a requirement for sample testing of the effectiveness and adequacy of the financial institution's policies, procedures and controls.

(vi) The Board must document its systems and controls (including policies and procedures) and clearly apportion responsibilities for the money laundering and financing of terrorism, and, in particular, responsibilities of the MLRO and CO.

(vii) According to the FSC Handbook, the board or senior management of the Company must establish documented systems and controls which:

a) undertake risk assessments of its business and its customers;
b) determine the true identity of customers and any beneficial owners and controllers;
c) determine the nature of the business that the customer expects to conduct and the commercial rationale for the business relationship;
d) require identification information to be accurate and relevant;
e) require business relationships and transactions to be effectively monitored on an ongoing basis with particular attention to transactions which are complex, both large and unusual, or an unusual pattern of transactions which have no apparent economic or lawful purpose;
f) compare expected activity of a customer against actual activity;
g) apply increased vigilance to transactions and relationships posing higher risks of money laundering and financing of terrorism;
h) ensure adequate resources are given to the CO to enable the standards within the FSC Handbook to be adequately implemented and periodically monitored and tested;
i) ensure procedures are established and maintained which allow the MLRO and the Deputy MLRO to have access to all relevant information, which may be of assistance to them in considering suspicious transaction reports ("STRs");

Control Systems

To assist in the proper monitoring and control of suspicious transactions, the Board should set up a control system by appointing a Compliance Officer who shall have a direct reporting line to the Board. The latter will report to the Board on a quarterly basis on issues relating to money laundering and other related subjects including external laws, rules, codes, regulations.

Transaction Examination

Reasonable steps would be taken to allow the identification of suspicious transactions. In the recognition of suspicious transactions, employees should be particularly aware of two essential elements:

(a) the usual nature of the client's business (Know Your Client – KYC); and
(b) the usual type of business carried out by the Company (Know Your Business – KYB) principles.

Suspicion should be aroused where the two principles do not match. Employees should report all transactions that they suspect to be linked to criminal activity. They are not allowed to turn a blind eye to the transaction as it might amount to an offence under the FIAMLA.

Money Laundering Reporting Officer

Pursuant to Regulation 27 of FIAMLR 2018, the Company must establish, document, maintain and operate reporting procedures that shall:

(i) enable all its directors or, as the case may be, partners, all other persons involved in its management, and all appropriate employees to know to whom they should report any knowledge or suspicion of money laundering and terrorism financing activity;

(ii) ensure that there is a clear reporting chain under which that knowledge or suspicion will be passed to the Money Laundering Reporting Officer;

(iii) require reports of internal disclosures to be made to the Money Laundering Reporting Officer of any information or other matters that come to the attention of the person handling that business and which in that person's opinion gives rise to any knowledge or suspicion that another person is engaged in money laundering and terrorism financing activity;

(iv) require the Money Laundering Reporting Officer to consider any report in the light of all other relevant information available to him for the purpose of determining whether or not it gives rise to any knowledge or suspicion of money laundering or terrorism financing activity;

(v) ensure that the Money Laundering Reporting Officer has full access to any other information that may be of assistance and that is available to the reporting person; and

(vi) enable the information or other matters contained in a report to be provided as soon as is practicable to the FIU where the Money Laundering Reporting Officer knows or suspects that another person is engaged in money laundering or terrorism financing activities."

The primary duty of the MLRO will be receiving and evaluating internal STR and where appropriate, filing the STR with the FIU. In the absence of the MLRO, appointment of Deputy MLRO must be duly notified to the FSC, and he/she is expected to fulfil similar duties as that of the MLRO.

Compliance Officer

As part of its compliance arrangements, the Company is responsible for appointing a CO who is responsible for the implementation and ongoing compliance of the Company with internal programs, controls and procedures in accordance with the requirements of the FIAMLA, FIAMLR 2018 and FSC Handbook.

The CO shall have the following functions:

a) ensuring continued compliance with the requirements of the FIAMLA, FIAMLR 2018, and FSC Handbook subject to the ongoing oversight of the Board and senior management;
b) undertaking day-to-day oversight of the program for combating money laundering and terrorism financing;
c) regular reporting, including reporting of non-compliance, to the Board and senior management;
d) contributing to designing and implementing the AML/CFT framework for the Company;

e) preparing and presenting annual compliance reports or such other periodic reports as deemed necessary on the adequacy/shortcomings of internal controls.

A full-time employee of the company will be employed in Mauritius to conduct some compliance functions related to AML/ CFT, inter alia, customer identification and verification, performing enhanced due diligence, screening and risk profiling.

Company Administrator

The Company has entered into an Administration Agreement with the appointed Administrator, which will act as the Administrator of the Company. The Administrator must be licensed with the FSC as a Management Company and supervised by the FSC in terms of its AML/CFT controls.

The Administrator will perform:

- Certain administrative functions;
- Accounting;
- Registrar;
- Transfer agency services for the Company (e.g., Customer / Shareholder register); and
- Transactional record keeping

Where the Administrator outsources certain of its functions to an Administrator Agent, the Administrator enters into an administration agreement with the Administrator Agent, however, the approval for the use of the Administrator Agent to conduct functions of the Administrator must be approved and vetted by the Board first.

Outsourcing of compliance-related functions

The Company may outsource some or all of its compliance functions related to AML/ CFT to a third party which shall ensure that the Company implements its program for combating money laundering and terrorism financing and managed all potential risks relating thereto in accordance with its own policies and procedures.

Prior to outsourcing the compliance-related functions, the Company shall assess the policies and processes of the third party.

Risk Based Approach

Aims of adopting a risk-based approach

A risk-based approach towards the prevention and detection of ML and TF aims to support the development of preventative and mitigating measures that are commensurate with the ML and TF 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 financial institution should:

(a) understand its ML and TF risks; and
(b) have in place effective policies, procedures, and controls to:
(i) identify,
(ii) assess,
(iii) understand
(iv) mitigate,
(v) manage, and
(vi) review and monitor, those risks in a way that is consistent with the requirements of section 17 of the FIAMLA 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 ML and TF, 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.

Through the business risk assessments and determination of a risk appetite, the Company can establish the basis for a risk-sensitive approach to managing and mitigating ML and TF risks. 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.

Business Risk Assessment

The Company must, under Section 17(1) of the FIAMLA identify, assess, understand and monitor that person's money laundering and terrorism financing risks. As explained in the FSC Handbook, a risk assessment 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 of ML and TF 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 business risk assessments are designed to assist the Company in making such an assessment and provide a method by which the Company can identify the extent to which its business and its products and services are exposed to ML and TF. Good quality business risk assessments are therefore vital for ensuring that Company's policies, procedures and controls are proportionate and targeted appropriately.

Company records and documents its risk assessment in order to be able to demonstrate its basis. The assessment is undertaken as soon as reasonably practicable after the Company commences business and regularly reviewed and amended to keep it up to date. This risk assessment is reviewed at least annually and the review is documented to evidence that an appropriate review has taken place.

Any risks that have been identified are properly mitigated by policies, procedures and controls. The Company also documents the mitigating factors and controls put in place to provide an audit trail of how the assessed risks have been mitigated.

Section 17(2) of the FIAMLA requires businesses to assess 6 key areas when undertaking the business risk assessment 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 business risk assessment.

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 ML/TF. Appropriate action should be taken to mitigate the risks that have been identified.

The Company has adopted a Business Risk Assessment Framework which is found in an ancillary document to this Manual.

Customer Risk Assessments

A customer risk assessment estimating the risk of ML/TF 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. The customer risk assessment may have to take into account that not all CDD and relationship information might have been collected yet. It is a living document that is revisited and reviewed, as and when more information about the customer and relationship is obtained. The customer risk assessment is done on categories of clients (risk buckets), and it is not necessary to individually risk rate each client should the Company deem it appropriate.

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

- 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 is exercised under a risk-based approach. Being identified as carrying a higher risk of ML/TF does not automatically mean that a customer is a money launderer or is financing terrorism. Similarly, identifying a customer as carrying a lower risk of ML/TF 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.

The Company has adopted a Customer Risk Assessment and Scoring Methodology which is found in an ancillary document to this Manual.

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.

Screening

Screening covers Sanction, PEP's and Adverse Media on the customers, Associated Parties, Beneficial Owner (''BO'') and all parties identified in the organizational and control structure. The Company shall ensure that clients, connected parties of clients and all natural persons appointed to act on behalf of clients are screened against these lists for the purpose of determining if there are any money laundering and terrorism financing risks in relation to the customers.

All new customers and their Associated Parties (including B.O., Immediate, Intermediate and Ultimate owners) must be screened up front through World Check and Internet Check, prior to on boarding. Existing customers must also be screened continuously. It is the Company's responsibility to ensure that ongoing screening is carried out on its applicants for business.

Sanctions Screening

Sanctions are measures imposed by governments across the world in response to a variety of international issues including terrorism and nuclear weapons proliferation. Sanctions make it an offence to do business with persons or entities listed in such sanctions. Sanctions lists are local and/or international lists of persons and entities with whom a business relationship may not be established.

These lists include the Office of Foreign Assets Control (OFAC), United Nations Security Council (UNSC) and European Union (EU) which are incorporated into the World Check Compliance screening performed by the Company.

Sanctions screening of all customers and where possible suppliers against applicable local and international sanctions and PEP lists shall be conducted. Where sanctions screening identifies a potential match, the result must be properly investigated in order to determine whether it is a positive match. In the event that the match and the MLRO/Deputy MLRO of the Company for investigation and potential onward reporting to the FIU.

Targeted Financial Sanctions

In order to ensure that employees are of the required standard of competence, which will depend on the role of the employee, the Company gives consideration to screening the employees against the UN's list of designated persons under terrorist and proliferation financing targeted financial sanctions, prior to, or at the time of, recruitment.

The Company also carries out periodic ongoing of its employees against the UN's list of designated persons under terrorist and proliferation financing targeted financial sanctions.

Section 23(1) of the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 (the "**UN Act**") provides that subject to the said Act, no person shall deal with the funds or other assets of a designated party or listed party, including –

(a) all funds or other assets that are owned or controlled by the designated party or listed party, and not just those that can be tied to –
    (i) a particular terrorist act, plot or threat;
    (ii) a particular act, plot or threat of proliferation;
(b) those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by the designated party or listed party;
(c) funds or other assets derived or generated from funds or other assets owned or controlled, directly or indirectly, by the designated party of listed party, and
(d) funds or other assets of a party acting on behalf of, or at the direction of, the designated party or listed party.

In addition, section 23(2) of the UN Act provides that where a prohibition is in force, nothing shall prevent any interest which may accrue, or other earnings due, on the accounts held by a listed party, or payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the prohibition, provided that any such interest, earnings and payments continue to be subject to the prohibition.

Where a party is listed pursuant to UNSCR 1737 and the listing continues pursuant to UNSCR 2231, or is listed pursuant to UNSCR 2231, the National Sanctions Committee may authorize the listed party to make any payment due under a contract, an agreement or an obligation, provided that the National Sanctions Committee:

(a) is satisfied that the contract, agreement or obligation was entered prior to the listing of such party;

(b) is satisfied that the contract, agreement or obligation is not related to any of the prohibited items, materials, equipment, goods, technologies, assistance, training, financial assistance, investment, brokering or services referred to in UNSCR 2231 and any future successor resolutions;
(c) is satisfied that the payment is not directly or indirectly received from, or made to, a person or entity
subject to the measures in paragraph 6 of Annex B to UNSCR 2231; and
(d) has, 10 working days prior to such authorization, notified the United Nations Sanctions Committee of its intention to authorize such payment.

In addition, any person who holds, controls or has in his custody or possession any funds or other assets of a designated party or listed party shall immediately notify the National Sanctions Secretariat of –

(a) details of the funds or other assets against which action was taken in accordance with subsection (1);
(b) the name and address of the designated party or listed party;
(c) details of any attempted transaction involving the funds or other assets, including –
(d) the name and address of the sender;
(e) the name and address of the intended recipient;
(f) the purpose of the attempted transaction;
(g) the origin of the funds or other assets; and
(h) where the funds or other assets were intended to be sent.

Any person who fails to comply with Section 23 (1) or (2) shall commit an offence and shall, on conviction, be liable to a fine not exceeding 5 million rupees or twice the amount of the value of the funds or other assets, whichever is greater, and to imprisonment for a term of not less than 3 years.

Section 24(1) of the UN Act relating to prohibition on making funds or other assets available to designated party or listed party available, provides that subject to the UN Act, no person shall make any funds or other assets or financial or other related services available, directly or indirectly, or wholly or jointly, to or for the benefit of –

(a) a designated party or listed party;
(b) a party acting on behalf, or at the direction, of a designated party or listed party; or
(c) an entity owned or controlled, directly or indirectly, by a designated party or listed party.

The Company has adopted an Economic Sanctions Policy which is found in an ancillary document to this Manual.

Independent Audit

Regulation 22 (1) (d) of the FIAMLR 2018 provides that every reporting person shall implement programs against money laundering and terrorism financing having regard to the money laundering and terrorism financing risks identified and the size of its business, which at a minimum shall include an independent audit function to review and verify compliance with and effectiveness of the measures taken in accordance with the FIAMLA and the FIAMLR 2018.

An AML/CFT independent audit is a vital element of any effective compliance programme for the Company. By virtue of the FIAMLA and FIAMLR 2018, there is a statutory obligation on every

company to have in place an audit function, which will allow the reporting entity to evaluate its AML/CFT programme and to ascertain whether the established policies, procedures, systems and controls are adapted with the money laundering and terrorism financing risks identified. The objective of an independent audit is to form a view of the overall integrity and effectiveness of the AML programme, including policies, procedures and processes.

Conducting a successful independent audit enables the Company to ensure that its policies, procedures and controls remain up to date, recognise deficiencies in regulatory compliance system and develop ways to remediate the breaches in order to be compliant with the prevailing legislation.

Scope of independent audit

In line with international best practices, the independent audit exercise should be risk-based. Independent audit is the Company's final line of defence; therefore, it is vital to ensure that the AML/CFT independent audit is tailored to the Company's risks.
The scope of the independent audit exercise is mainly a verification of the AML/CFT risk faced by the Company.

Typically, every independent audit should mandatorily test compliance in the following non-exhaustive areas:

- AML/CFT policies and procedures;
- Internal Risk Assessment;
- Risk Assessment on the use of third-party service providers (Outsourcing);
- Compliance Officer function and effectiveness;
- MLRO function and effectiveness;
- Implementation and Effectiveness of Mitigating Controls, including customer due diligence and enhanced measures;
- AML/CFT Training;
- Record Keeping Obligations;
- Targeted Financial Sanctions; and
- Suspicious Transaction Monitoring and Reporting.

If the Company relies on automated systems or manual processes to implement its AML/CFT programme, the reliability of these systems and processes should also be considered during the independent audit on a risk-basis.

Choosing the Audit Professional

Regulation 22 (1) (d) of the FIAMLR 2018 requires the audit process to be carried out independently. This implies that the person or firm conducting the audit should be independent and must not be involved in the development of the Company's AML/CFT risk assessment, or the establishment, implementation or maintenance of its AML/CFT programme.

The audit function should therefore be independent of, and separate from the operational and executive team dealing with the AML/CFT processes of the Company. An independent audit review may be conducted by an internal or external audit professional.

The person or firm conducting the audit should have the necessary skills, qualifications, relevant experience of the audit process, have a proper understanding of the FIAMLA and its supporting regulations as well as sufficient knowledge of the Company industry. In order to ensure that the audit is properly conducted as required under the FIAMLA and FIAMLR 2018, the audit professional needs to provide quality recommendations, so that the Company can use the findings and recommendations to improve upon deficient areas.

Assessing the "independence" of the audit professional.

In all cases, the Company must be satisfied and able to demonstrate that the person or the firm undertaking the audit is adequately independent from the area of the business function responsible for risk assessment and AML/CFT programme, and ensure that there are no conflicts of interest. Therefore, the independent audit may be conducted by an in-house audit professional not involved in the development and implementation of the AML/CFT programme or outsourced to external accountants or independent consultants duly regulated or registered by relevant competent authorities.

When sourcing an external audit professional to conduct the audit, the Company should conduct some level of due diligence as listed in Section 13.3 to confirm the proposed or selected professional candidate has the requisite competence. The criteria considered by the Company when assessing the independence and relevant experience of the external audit professional to effectively perform the audit, should be properly documented and shall be made available to the Commission upon request.

In order to assess the independence of the audit professional, the Company should ensure that the following non-exhaustive pertinent areas are addressed:

- Was the audit professional involved in the development of the entity's risk assessment? Or the creation, implementation or maintenance of the AML/CFT programme?
- Does the audit professional have financial interest in the business? If yes, would their interests be harmed by the results of the audit, or could there be influence over the audit outcome?
- Does the audit professional have any relationship with any shareholder, director, senior management and or employees?

Frequency of the Independent Audit

The frequency and extent of the review should be commensurate with the company's size, nature, context, complexity and internal risk assessment.

The Company should consider the appropriateness and effectiveness of its compliance arrangements and its policy for the review of compliance at a minimum annually, or whenever material changes to the Company or legislative and regulatory obligations occur. However, the Company can determine for itself the frequency to have its audits conducted. The greater the AML risk of the Company and of the rate of change of the Company's business, the greater should be the frequency of audit.

For any business that does not have clients during the reporting period, a company must ascertain the frequency to conduct its independent audit. It may be appropriate that the audit cycle be extended if the Company has no clients and no clients have been onboarded or exited since the previous independent audit is conducted.

For a company that is in process of being wound up, it is recommended that at least one final independent audit is carried out until the Company is no more considered as a reporting entity under the FIAMLA.

The basis for the audit frequency must be clearly articulated in the Company's audit policy and scope.

Key components of the AML/CFT programme

The independent audit report must express views on whether the AML/CFT risk assessment and the AML/CFT programme comply with the requirements of FIAMLA and supporting legislations and whether the programme is functioning effectively in practice as required and intended, and has been over the course of the period. The independent audit will involve obtaining a good understanding of the Company's business, reviewing relevant core documents, file testing, testing of the live application of policies and procedures, and interviewing a cross-section of players. The audit process must have sufficient depth and breadth to support the findings and to make the report worthwhile.

Within the framework of the AML/CFT programme itself, the independent audit shall inter alia:
- address the adequacy of AML/CFT risk assessment, including whether it addresses the specific business activities of that particular company;
- test compliance of the Company's AML/CFT programme, policies and procedures with the FIAMLA, FIAML Regulations 2018, and the AML/CFT Handbook and a general review of the effectiveness of the compliance function considering the risks identified through the risk assessment;
- assess the employees' adherence to the AML policies and procedures;
- assess employees' knowledge of the AML/CFT laws, regulations, guidance, and policies & procedures;
- examine the adequacy of Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) policies, procedures and processes, and whether they comply with higher-level internal requirements in the Company.

This may include considering the adequacy of onboarding paperwork and considering the adequacy of enhanced measures against the findings of the risk assessment;
- conduct appropriate customer file testing, with particular emphasis on high-risk operations (products, service, customer and geographical locations);
- examine the adequacy of the policies and procedures as well as the processes for identifying and reporting suspicious transactions promptly;
- if an automated system is not used to identify or aggregate large transactions, the audit should include sample test of how the compliance officer conducts monitoring;
- conduct appropriate transaction file testing, including a review of 'not filed' (closed as not suspicious) internal suspicious transactions reports, to determine the adequacy, completeness and effectiveness of the STR filing process;
- examine the adequacy of the policies and procedures as well as the processes for screening for targeted financial sanctions as well as implementing prohibitions, freezing assets, and reporting to competent authorities;
- review how the Company is screening for targeted financial sanctions without delay when onboarding clients or conducting transactions and when the lists are updated (within hours), and the appropriateness of periodic screening frequency;
- conduct appropriate testing of TFS screening records, including a review of false positives, to determine the adequacy, completeness and effectiveness of the TFS process;

- examine the integrity and the accuracy of the management information systems use in the AML compliance programme; and
- assess training adequacy including its comprehensiveness, accuracy of materials, training schedule and attendance tracking.

Overall, the audit professional should decide whether the audit coverage and frequency are appropriate to the risk profile of the Company.

Audit outcome, report and recommendations

The audit will result in a signed and dated written report by the audit professional to ensure that the audit programme:

- covers all relevant components of the compliance programme as required under FIAMLA and relevant regulations;
- was adequate and effective throughout a specified period;
- identifies areas where the Company did not meet minimum legal or regulatory standards, and include actions that are required to rectify non-compliance as well as identifying areas for recommended changes in behaviour and practice to improve the effectiveness of the AML/CFT programme's implementation. This includes an indication of where there are potential failings and a recommended course of action.

A key element of the whole audit process is effective follow-up. Failure to address recommendations and findings of previous audits should be red flagged to the board or audit committee and will be in any regulatory inspection. The findings of the independent audit report, highlighting recommendations and deficiencies, should be reported to senior management and to the board of directors.

It is the responsibility of the board of directors of the Company to take appropriate corrective actions to remediate any issues identified in the independent audit report within the specified timelines.

Filing to the Financial Services Commission

The Company is not required to file their independent audit report with the FSC periodically. However, the Company shall file its independent audit report for a specified period, upon the request of the FSC .
All independent audit documentation, including, *inter alia*, work plan, audit scope, transaction testing, should also be properly documented and shall be made available to the FSC upon request.

The FSC may *inter-alia*, request the following information:

(i) whether the Company has adequate policies and procedures in place for independent audit exercise;
(ii) what AML/CFT issues have been identified;
(iii) what are the controls and procedures in place to ensure that all risks identified are remediated in a timely manner;
(iv) when the Company has conducted its last independent audit;
(v) when the next independent audit exercise would be scheduled;
(vi) whether, from a corporate governance perspective, the Company is considering of rotating the audit professional after performing audit after a specific number of years, as it deems appropriate.

Ongoing monitoring for PEP

Once a business relationship has been established with a PEP, on-going monitoring must be conducted on all related transactions to ensure that they are in line with the customer's source of funds and wealth and original account mandate. This can be achieved by requesting for additional information to understand the purpose of a transaction and verifying the provenance of the source of funds and where required, to request for evidentiary documents such as agreements, invoices, bank statements, etc.

Furthermore, quarterly World Check and Internet Check must be conducted on the PEP and evidence of such screening kept on records. Annual reviews must be conducted on all customers identified as PEPs and approved by Board / Senior Management.

The following information and documentation must be reviewed/reconfirmed/updated when conducting an annual review of a PEP investor:

- All KYC information;
- The relevance of the EDD conducted initially including reconfirmation of the customer's source of funds and source of wealth;
- Where adverse information such as ongoing litigation or regulatory proceedings were noted as part of the on-boarding information, further checks must be undertaken to ascertain any outcomes or obtain updated information;

Information obtained from the customer may be compared against additional independent sources in order to verify the accuracy of the information. The formal decision and reasons to either maintain or terminate the PEP relationship must be documented.

Factors to consider in establishing/maintaining/terminating a customer relationship with a PEP

The following are factors, which should be considered in deciding whether to establish/ maintain/terminate a customer relationship with a PEP:

- funding of the account: are the Company's in the account in line with the customer's source of funds and wealth and original account mandate;
- is there a history of suspicious or unexplained transactions;
- is the customer responsive to requests for up to date information?

There should be a detailed consideration of the rationale for establishing, maintaining, or terminating the business relationship with the PEP.

[Note – where a customer has been accepted and the said customer or its beneficial owner or its associate or its family member is subsequently found to be, or subsequently becomes a PEP, appropriate EDD and Company Board's approval should be obtained as per above in order to continue such business relationships.]

Connected persons that are PEPs

'Connected persons' will include underlying principals such as beneficial owners and controllers.

The Company must apply appropriate EDD measures on a risk-sensitive basis where an applicant for business or customer (or any connected person, such as a beneficial owner or controller) is a PEP, and must ensure that they operate adequate policies, procedures and controls to comply with this requirement.

The Company must:

- Develop and document a clear policy on the acceptance of business relationships or one-off transactions with such persons, and ensure that this is adequately communicated;
- Obtain and document the approval of senior management prior to establishing relationships with such persons;
- Where such persons are discovered to be so only after a relationship has commenced, thoroughly review the relationship and obtain senior management approval for its continuance; and
- Apply EDD measures to establish the source of funds and source of wealth of such persons.

Verification of source of funds and source of wealth

The source of funds and source of wealth are required to be verified to demonstrate a thorough understanding of the source of the initial and ongoing funds and wealth that will pass through the customer's account/product held at the Company. Where initial funding is provided by third parties, the Company should ensure that the relationship between the parties is fully documented and a rationale for such a relationship is recorded and analyzed. If there is no proven rationale for the existence of such a relationship, further due diligence is required.

The source of funds and source of wealth of the PEP must be verified in accordance with the source of funds and source of wealth requirements applicable to that PEP.

Customer Risk Profiling

The Company must identify and assess its potential exposure to inherent ML, TF and sanctions risks introduced as a result of entering into a business relationship with a customer. The Company assesses business relationship risks through a Customer Risk Profiling Toolkit.

The Company will take a number of factors into consideration including but not limited to the following:

- Nature and type of Customer;
- Customer's Nationality (Individual) or Registration Country (Corporate)
- Geographical location of the customer's residence / base of activity;
- Customer's source of funds;
- Customer's Activity;
- Transaction Frequency;
- Product type
- High Risk Indicators such as: a) Incomplete CDD, b) Dealing with PEP, c) Dealing with Sanctioned countries, d) Unsupported bank transactions, e) World Check Hit or any adverse info from media or internet, f) EIC or Omnibus Exceptions (not meeting FSC's minimum requirements).

Risk profiling is applicable to:

- New Customers (at on-boarding stage); and

- Existing Customers.

The following Risk Profiling Classification & Review Date:
- High risk: every 12 months;
- Medium risk: every 24 months; and
- Low risk: every 36 months.

The Company is required to review its customer risk profiling methodology to ensure the customer risk categories remain relevant and reflective of the real risk that the Company is exposed to as a result of its customer relationships.

Third Party Reliance

The Company may rely on its administrator, IQ EQ Fund Services (Mauritius) Ltd ("**IQ-EQ**") to complete certain CDD measures. IQ-EQ is regulated, supervised, monitored and is subject to CDD and record keeping requirements pursuant to regulations of the FIAMLA. The Company is aware that the ultimate responsibility for CDD measures remains with the Company.

Pursuant to Chapter 8 of the FSC Handbook, a financial institution may rely on relevant third parties to complete certain CDD measures, provided that there is a contractual arrangement in place with the third party. Where reliance is placed on a third party for elements of CDD, the financial institution must ensure that the identification information sought from the third party is adequate and accurate. The CDD information has to be submitted immediately in line with section 17D of the FIAMLA upon onboarding although the documents can be provided upon request at a later date. Where such reliance is permitted, the ultimate responsibility for CDD measures will remain with the financial institutions relying on the third party.

In a third-party reliance scenario, the third party should be regulated, supervised and monitored and subject to CDD in line with section 17C of the FIAMLA and record keeping requirements pursuant to section 17F of the FIAMLA and Regulation 21 of the FIAMLR 2018 which provides for third party reliance. When reliance is placed on a third party that is part of the same financial group, the financial institution must ensure that the group applies the measures as applicable to regulation 21(4) of the FIAMLR 2018.

Moreover, the financial institution needs to be aware on the level of the country risk when determining in which country (ies) the third party can be based, countries with strategic deficiencies in the fight against money laundering and the financing of terrorism, e.g., those identified by the FATF as having strategic deficiencies. A high-risk country can also be those countries that are vulnerable to corruption and which are politically unstable, the above examples are not exhaustive.

Reliance may only be placed on third parties to carry out CDD measures in relation to the identification and verification of a customer's identity and the establishment of the purpose and intended nature of the business relationship. Third parties may not be relied upon to carry out the ongoing monitoring of dealings with a customer, including identifying the source of wealth or source of funds. The FSC recommends that regular assurance testing is carried out in respect of the third-party arrangements, to ensure that the CDD documents can be retrieved without undue delay and that the documentation received is sufficient pursuant to section 17(2)(v) of the FIAMLA.

Financial institutions should take steps to ensure that any existing third-party reliance arrangements comply with the applicable AML/CFT legislation in this regard. It is suggested that, where third party reliance arrangements are in place, reporting entities (e.g., funds) receive a report from the administrator about the arrangements that meets those requirements and that the report details the outcome of the testing carried out.

The Company shall, pursuant to section 17H of the FIAMLA, with respect to business relationships or transactions involving a high-risk country, apply such enhanced CDD measures as may be prescribed.

In addition, the Company shall, where applicable and proportionate to the risks, apply one or more of the following additional mitigating measures to persons and legal entities carrying out transactions involving a high-risk country:

(a) The application of additional elements of enhanced due diligence;
(b) The introduction of enhanced relevant reporting mechanisms or systematic reporting of financial transactions;
(c) The limitation of business relationships or transactions with natural persons or legal entities from the countries identified as high-risk countries.

Monitoring Accounts for Suspicious Activity

We will manually monitor a sufficient amount of 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 below. We will look at transactions, including trading and wire transfers, in the context of other account activity to determine if a transaction lacks financial sense or is suspicious because it is an unusual transaction or strategy for that customer. The Compliance Officer or his or her designee will be responsible for this monitoring, will document when and how it is carried out, and will report suspicious activities to the appropriate authorities. Among the information we will use to determine whether to file a report are exception reports that include transaction size, location, type, number, and nature of the activity. We will create employee guidelines with examples of suspicious money laundering activity and lists of high-risk clients whose accounts may warrant further scrutiny. Our CO will conduct an appropriate investigation before a STR is filed.

Emergency Notification to the Government by Telephone

When conducting due diligence or opening an account, we will immediately call law enforcement when necessary, and especially in these emergencies: we discover that a legal or beneficial account holder or person with whom the account holder is engaged in a transaction is listed on or located in a country or region listed on the OFAC list, an account 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, or we have reason to believe the customer is about to use the funds to further an act of terrorism.

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.

Responding to Red Flags and Suspicious Activity

When a member of the Company detects any red flag he or she will investigate further under the direction of the CO. This may include gathering additional information internally or from third-party sources, contacting the government or filing a Form SAR-SF and STR.

Where a suspicion exists on any transaction, the CO must immediately report the matter to the MLRO. It is vital not to inform any 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.

Suspicious Transactions and Reporting

Recognition of Suspicious Transactions

Section 2 of the FIAMLA 2002 defines a suspicious transaction as "…. *a transaction which* –

(a) gives rise to a reasonable suspicion that it may involve -
  (i) the laundering of money or the proceeds of any crime; or
  (ii) *funds linked or related to, or to be used for, the financing of terrorism or proliferation financing or, any other activities or transaction related to terrorism as specified in the Prevention of Terrorism Act or under any other enactment, whether or not the funds represent the proceeds of a crime*;
(b) is made in circumstances of unusual or unjustified complexity;
(c) appears to have no economic justification or lawful objective;
(d) is made by or on behalf of a person whose identity has not been established to the satisfaction of the person with whom the transaction is made; or
(e) gives rise to suspicion for any other reason."

The word "transaction" is also defined in section 2 of FIAMLA, as follows –

(a) opening an account, issuing a passbook, renting a safe deposit box, entering into a fiduciary relationship or establishing any other business relationship, whether electronically or otherwise; and
(b) a proposed transaction or attempted transaction."

This definition is not exhaustive.

The assessment of suspicion should be based on a reasonable evaluation of different factors, including the knowledge of the Client's business, financial history, unusual pattern of activity, risk profile, background and behavior. All circumstances surrounding a transaction should be reviewed. It follows that an important precondition for recognition of a suspicious transaction or activity is that the employees of the Company must know enough about the business relationship to recognize that a transaction or activity is unusual.

In case of suspicion, an employee is not expected to know the exact nature of the underlying criminal offence (called the predicate offence), or that the particular funds were those arising out of the crime or being used to finance international terrorism. The simple rule is, where a transaction raises any suspicion, the employee should as a first step request more information from the customer about the circumstances surrounding the transaction. He must decide if the explanation received is reasonable and legitimate and if not, report the transaction to the MLRO.

Internal Reporting of Suspicious Transactions

It is a statutory obligation on all employees to report suspicious transactions promptly and directly to the MLRO or to his deputy in his absence. This should normally be done via an Internal STR Form ("ISF"),

In urgent circumstances, an internal STR may be reported to the MLRO verbally and followed by the ISF. Failure to report suspicious transactions will constitute a breach of the FIAMLA and may entail criminal sanctions and interference with the preparation or submission of an internal STR may lead to disciplinary sanctions.

The MLRO shall be of sufficiently senior status and shall have relevant and necessary competence, authority and independence. The contact details of the MLRO and those of the Deputy MLRO are provided below:

	MLRO	**Deputy MLRO**
Name	Sandev Singh Soobagrah	Kishen Hurhinidee
Email	Dan.Soobagrah@iqeq.com	Kishen.Hurhinidee@iqeq.com
Telephone	212 9800	212 9800

All suspicions reported to the MLRO will be recorded in writing, even if the suspicion is reported verbally. The internal STR should include full details of the Client and a full statement as to the information giving rise to the suspicion. The MLRO will acknowledge receipt of the internal STR and, at the same time, provide a reminder of the obligation to do nothing that might prejudice enquiries – that is, ***'tipping off'*** the customer which is a criminal offence under the FIAMLA.

The MLRO will validate all internal STRs before submissions to the FIU and make sure that reports are not made in bad faith, maliciously and without reasonable grounds.

Reporting of Suspicious Transactions to the FIU

Once the MLRO receives an ISF from the relevant staff member, he will determine whether the information contained in the internal STR gives rise to a suspicion that a Client is engaged in ML and/ or TF. In this respect, the MLRO shall have unfettered access to any or all information which he may need in considering his report. In making his judgment, the MLRO will consider all relevant information that has been made available to him.

If, after completing the review he believes that there is no fact(s) which can negate the suspicion, he has the obligation to report the transaction in writing to the FIU through the latter's online platform, goAML. If, on the other hand, the MLRO does not find it appropriate to report a transaction to the FIU, he will document the reasons for not doing so. This information may be required to supplement the initial report or as evidence of good practice and best endeavors if, at some future dates, there is an investigation and the suspicions are confirmed. On-going communication between the MLRO and the reporting staff is important.

The MLRO is expected to act autonomously, promptly, honestly and reasonably, and to make any determination in good faith.

Reporting Obligations and Offences

Section 14(1) of the FIAMLA provides that "*Notwithstanding section 300 of the Criminal Code and any other enactment, every reporting person or auditor shall, as soon as he becomes aware of a suspicious transaction, make a report to FIU of such transaction not later than 5 working days after the suspicion arose.*"

Pursuant to section 14(3) of the FIAMLA -

"*Where a reporting person or an auditor –*

(a) becomes aware of a suspicious transaction; or

(b) ought reasonably to have become aware of a suspicious transaction,

and he fails to make a report to FIU of such transaction not later than 5 working days after the suspicion arose he shall commit an offence and shall, on conviction,

be liable to a fine not exceeding one million rupees

and to imprisonment for a term not exceeding 5 years."

AML Record Keeping

Responsibility for AML Records and SAR Filing

Our Compliance Officer and his or her designee will be responsible to ensure that AML records are maintained properly and that SARs are filed as required. We will maintain AML records and their accompanying documentation for at least seven years. We will keep other documents according to existing BSA and other record keeping requirements.

Training Programs

The Company will develop ongoing employee training under the leadership of the AML Compliance Officer and senior management in accordance with applicable laws. Our training will occur on at least an annual basis. It will be based on our Company's size, its customer base, and its resources.

Our training will include, at a minimum: how to identify red flags and signs of money laundering that arise during the course of the employees' duties; what to do once the risk is identified; what employees' roles are in the Company's compliance efforts and how to perform them and the Company's record retention policy. We will develop training in our Company, or contract for it. Delivery of the training may include educational pamphlets, videos, intranet systems, in-person lectures, and explanatory memos. We will maintain records to show the persons trained, the dates of training, and the subject matter of their training.

We will review our operations to see if certain employees, such as those in compliance, margin, and corporate security, require specialized additional training. Our written procedures will be updated to

reflect any such changes. Regular training will be provided to all employees on AML/CFT. All employees should attend the training sessions which will be delivered by the MLRO and/or Compliance Officer. The main objective of the training is to generate and maintain a satisfactory awareness level and vigilance that would help identify any suspicious transaction.

Business Continuity Plan

Background

While it is recognized 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.

Business Description

The Company was incorporated in Mauritius on 09 November 2021 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.

Company Policy

Our 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.

Significant Business Disruptions (SBDs)

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 in our Key Man Policy and work in conjunction with our administrator.

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.

Approval and Execution Authority

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

Plan Location and Access

Our Company will maintain copies of its 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, which is kept on the Company's Dropbox in the Company Compliance folder.

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 and utilize their VPNs.

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

Our Company maintains its primary hard copy books and records and its electronic records at:

C/o IQ EQ Fund Services (Mauritius) Ltd
33 Edith Cavell Street
Port-Louis, 11324, Mauritius
Phone: (230) 212 9800

IQ EQ Fund Services (Mauritius) Ltd is responsible for the maintenance of these books and records. Our Company maintains the following document types and forms that are not transmitted to our brokerage firm: Investment Policy Statements, Client Contracts and other related documents.

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

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.

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.

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.

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

Orderly Unwinding Procedures

In the event that the entire investment committee is incapacitated, the administrator will work in consultation with the CCO 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.

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.

Supervisor Approval

Approve the Company's Business Continuity Plan (BCP) program by signing below.
I have approved this Business Continuity Plan as reasonably designed to enable our Company to meet its obligations to clients in the event of a Significant Business Disruption.

Signed:

Officer Name and Title:	
Supervisor Signature	**Date**

Definitions

1. "**Access Person**" includes any supervised person who has access to nonpublic information regarding any clients' purchase or sale of securities, or nonpublic 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 nonpublic. All of the Company's directors, officers, and partners are presumed to be access persons.
2. "**Company**" means MGF and vice versa.
3. 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.
4. "**Conflict of Interest**": for the purposes of this Code of Ethics, 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.
5. "**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.
6. "**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.
7. "**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.
8. "**Purchase or sale of a Covered Security**" includes, among other things, the writing of an option to purchase or sell a Covered Security.
9. "**Reportable security**" The Rule considers all securities reportable except for the following:
    a. Direct obligations of the Government of the United States;
    b. Bankers' acceptances, bank certificates of deposit, commercial paper and high-quality short-term debt instruments, including repurchase agreements;
    c. Shares issued by money market funds;
    d. Shares issued by open-end funds other than reportable funds; and
    e. Shares issued by unit investment trusts that are invested exclusively in one or more open-end funds.
10. "**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.

Client Due Diligence Checklist

Customer Due Diligence ('CDD') documents in English or French or translation certified by a qualified translator shall be provided in original or as certified true copies (by lawyer, notary, actuary, banker, accountant and police indicating the name, position and contact details) on the Investors of the Fund as follows:

A. For Individual:

- Signed CV
- Valid passport (showing the name, date/place of birth, nationality, date of issue/expiry and signature of the holder)
- Proof of the individual's current address (e.g current utility bill), (current original bank statement or a recent original bank reference which includes the residential address)

B. For Corporate Body:

- Certificate of incorporation/formation documents
- Certificate of Good Standing
- Profile of the Corporate Body (including Name of Corporate Body, date/country of incorporation/formation, registered address, business address, issued capital, controlling shareholders, directors, business activities, financial highlights - total assets and total liabilities) [Specimen Provided]
- Authorization of any person who purports to act on behalf of the Corporate Body
- CDD documents on the ultimate controlling shareholder(s) of the corporate body.
- Controlling shareholders is any person who is entitled to exercise, or control the exercise of, 20% or more of the voting power at general meetings of the Company or one which is in a position to control the appointment and/or removal of directors holding a majority of voting rights at board meetings on all or substantially all matters. (Refer to List A or B)
- CDD documents on two of the directors of the corporate body (Refer to List A above)

C. For Trust:

- Certificate of registration, if applicable
- Trustee- registered office, place of business, license held and the authority by which the Trustees are regulated, if applicable. Please note that if the trustee is not regulated, then documents as listed in item B should be requested on the Trustee.
- Extracts of Trust Deed signed by the Trustees OR Profile of the Trust [Specimen Provided] (including. name of the Trust, date of establishment, type of Trust, an indication of assets value held by the Trust, names of settlor, contributor, beneficiaries and protector of the Trust)
- CDD documents on the settlor, contributor, beneficiaries and protector of the Trust (Refer to List A or B above)
- For discretionary trust, an undertaking from the Trustees that CDD documents on beneficiaries at the time of distribution will be made available to the Company

D. For Partnership

- Partnership deed
- Certificate of Registration/Establishment or Certificate of Good Standing of the Partnership and the General Partner
- Partnership profile (including Name of Partnership, Date/country of formation, registered address, business address, committed capital, Name of General Partners and list of significant Limited Partners (owning and controlling not less than 20% of the Partnership), business activities, financial highlights - total assets and total liabilities)
- Authorization of any person who purports to act on behalf of the Partnership

E. For Listed Entity or regulated financial service business

- License – listing/regulated status
- Audited account or annual report
- Authorization of any person who purports to act on behalf of the Corporate Body

Employee Attestation

I attest that I, a supervised person of the Company, have read, understood, and agree to comply with the rules in the Policies and Procedures Manual and Code of Ethics.

Signed:

Supervised Person Name		**Date**
Supervised Person Signature		
Supervisor Signature		