ASSETS GLOBAL LTD

Investment Dealer (Full-Service Dealer excl. Underwriting) License

INTERNAL POLICIES, PROCEDURES & CONTROLS MANUAL

MARCH 2023

PRIVATE & CONFIDENTIAL

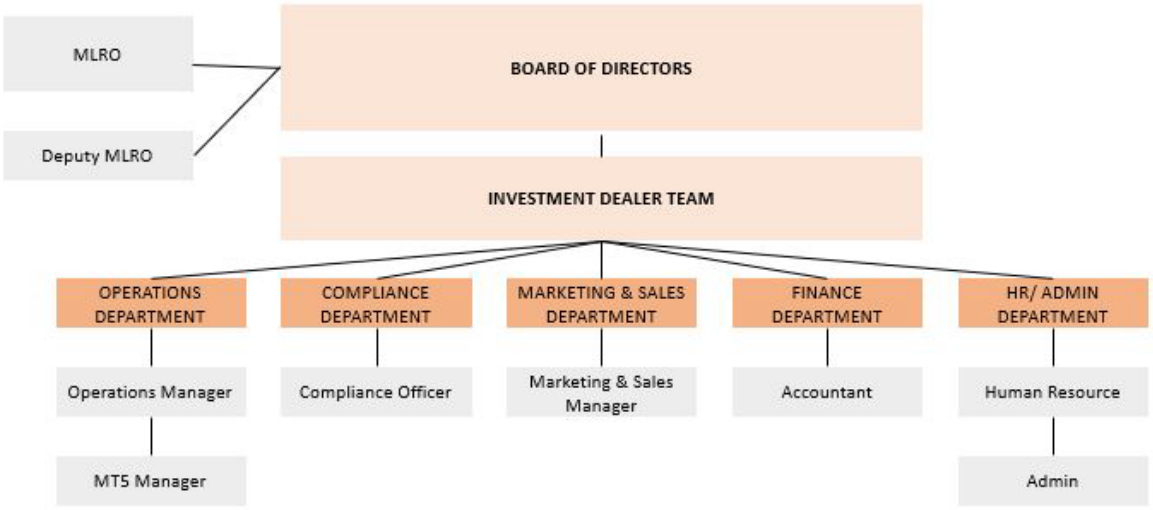
ASSETS GLOBAL LTD

ASSETS GLOBAL LTD

1. INTERNAL PROCEDURES & COMPLIANCE MANUAL

GENERAL OPERATIONAL AND INTERNAL PROCEDURES AND GUIDELINES

ORGANISATION STRUCTURE



Core Activities

The Marketing & Sales Personnel will assist the Investment Dealer Team in the following duties:

- Building long term relationships with its clients.
- Verifying client information and informing clients regarding account opening procedures and documentation requirements.
- Promoting the features and benefits of all products, services, promotions, and trading platforms to prospective clients.
- Following up on all existing clients to increase trading volumes.

The Finance Personnel will assist the Investment Dealer Team in the following duties:

- Providing support to clients on trading platforms, sending notifications about quotes and trade deals.
- Monitoring and reporting on clients' investments.
- Reporting cash and margin availability of clients' accounts.

PRINCIPLES FOR BUSINESS CONDUCT

The Company aims to deliver its services in line with international best practice. A set of principles as defined in the Code of Business Conduct by the Financial Services Commission has been identified by the Company and are as follows:

1. Integrity

It must observe high standards of honesty, integrity and fairness and ensure that all business transactions are carried out and recorded fairly and accurately to avoid misleading and deceptive acts or representations.

2. Skill, Care and Diligence

It must conduct its business with due skill, care and diligence. It must have in place appropriate safeguards, including appropriate staff training. The Company must also apply the "fit and proper" test for their officers and persons acting on their behalf.

3. Management and Control

It must take reasonable care to organize and control its affairs responsibly and effectively, with adequate risk management systems.

4. Financial Prudence

It must maintain adequate financial resources at all times and must comply with its licensing conditions.

5. Market Conduct

It must observe proper standards of market conduct.

6. Customer's Interests

It must pay due regard to the interests of its customers and treat them fairly.

7. Communications with Clients

It must pay due regard to the information needs of its clients and communicate information to them in a way which is timely, clear, fair and not misleading.

8. Conflicts of Interest

It must avoid situations of conflict of interests and in case conflict arises, it must ensure fair treatment of all their customers. Appropriate and frequent disclosures should be made where required.

9. Customers: Relationship of Trust

It must take reasonable care to ensure the suitability of its advice and discretionary decisions for any customer who is entitled to rely upon its judgment.

10. Clients' Assets

The Company must ensure that clients' assets are properly identifiable and segregated.

11. Relations with Regulators

It must deal with its regulators in an open and cooperative way and must disclose to the FSC appropriately anything relating to the Company of which the FSC would reasonably expect notice.

12. Terms of Business

It must ensure that its client and it are in full agreement about the nature, scope and terms of the services to be provided. It must ensure that its proposal best satisfy the needs of its client.

13. Dealing with Complaints

It must act promptly and do whatever is appropriate to resolve justified complaints.

14. "Know-Your-Customer Principle"

It shall be satisfied of the identity of its customer before engaging into any business relationship as required by the applicable laws. Policies and procedures shall be established to ensure that proper KYC principle is applied by the Company to combat money laundering and financing of terrorism.

15. Compliance

It must observe high standards of market conduct and must comply with all regulatory requirements applicable to the conduct of its business activities so as to promote the best interests of customers and the integrity of the market.

SEGREGATION OF FUNDS

The Company will open its principal bank account in Mauritius with separate Client Account and Corporate Account. The Company will ensure a proper segregation with respect to clients' funds which are to be kept separately from the Corporate Account at all times.

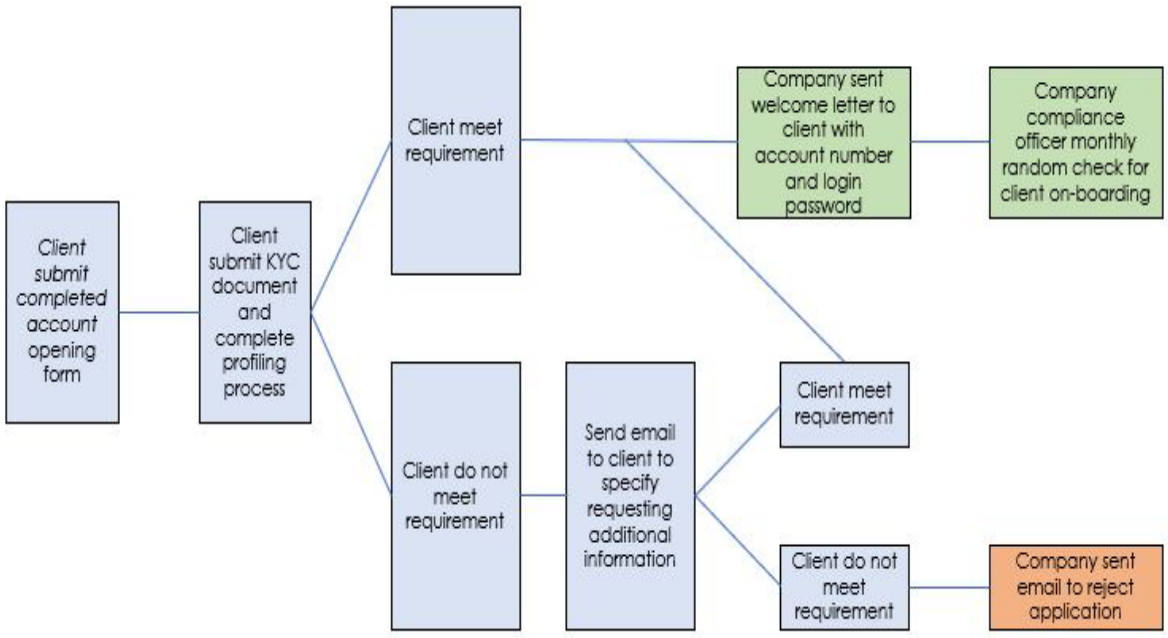
The Company keeps separate accounts for its own operational needs or portfolio management clients. The bank account for its operation is credited with all fees including management fee, interest income and other income as per the agreements it maintains with its clients. All operating expenses of the Company are paid from this account.

SHARING INFORMATION AND CONFLICTS OF INTEREST

The Company will do its best to manage conflicts of interest fairly, both between itself and its customers and between a customer and another client. All cases of conflicts of interest need to be reported to the Compliance Officer and Managing Director of the Company. The code of ethics of the Company dedicates a section on conflicts of interest.

Any sharing of information between the different teams of the Company will only occur in respect of the requirements of the above functions. Each team needs to ensure that there is no misuse and abuse of sensitive information by any of them and any other third party.

CLIENT ONBOARDING PROCESS



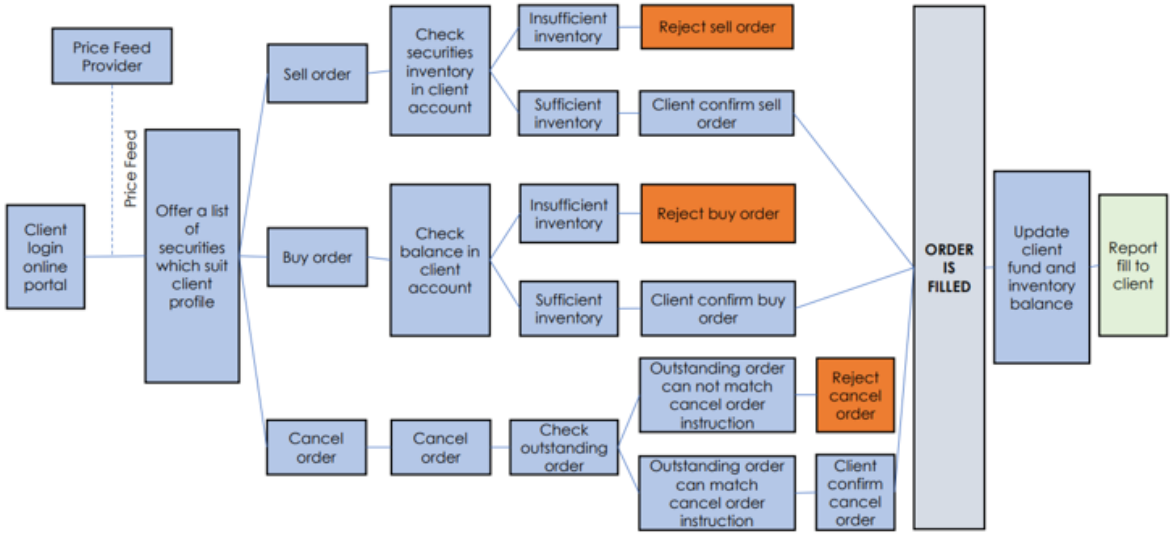
- Client requests or downloads from the Company's website an account opening form
- The client fills in and submits the client opening form together with his CDD documents
- Documents are sent to the Compliance team for the review of all documents
  - If documents are incomplete or missing, the client is contacted requesting same
    - If client reverts back with missing documents or information, same is resent to Compliance team for review. Compliance team will re-assess the client and will either accept or reject the client subject to the latter meeting the requirements of the Company and client is advised on same
    - If client does not revert back with missing documents or information, application is rejected and client is advised on same
  - If client meets requirement, the client is advised that the application has been successful and client is provided with a user name and password and is requested to fund the account by transferring the fund to the client account of the Company by wire transfer.
  - Once the fund is sighted in the client account of the Company, the Operations Manager activates the account.

Risk Profiling

All clients are required to complete a **Client Application Form** which requires the client to provide details on his sources of income, his accumulated wealth, risk appetite, investment objectives and investment horizon.

OPERATION PROCESS

Order Transmission & Transaction Flow Process



Client will have access to the platform through the username and password provided on completion of onboarding. For security measure the Investment Team and the Operations Manager will have access to the platform.

In the event, the online platform is down and temporarily not available, the clients are accorded with the possibility to have access to the trading desk through emails and telephone calls.

Portfolio Management Process

The process that the Company shall implement is as follows:

1. Profiling and due diligence of clients to identify risk behaviour, time horizon and investor needs
2. Conduct due diligence and obtain compliance approval
3. Sign the Discretionary Investment Management Agreement with clients
4. Decide on the amount to invest on each security based on the agreed asset allocation and investment strategy
5. Implement the investment process: place orders with different dealers/ stock broking company and follow up orders
6. Prepare portfolio reports for Clients

The management of portfolios will be on a discretionary basis.

PREVENTION OF MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION FINANCING

Our internal processes and procedures have been designed in such a way as to ensure:

- A framework is in place to cover proper management, systems and controls and other related matters.
- Periodical review of all the applicable laws, rules and standards, including keeping up to date with developments in the applicable laws, rules and standards and advising Management accordingly.
- Establishing written guidance to staff on the appropriate implementation of the laws, rules and standards through policies and procedures and other documents such as compliance manuals, internal codes of conduct and practice guidelines.
- Monitoring the compliance risk within the company by performing regular and comprehensive compliance risk assessment and testing, and reporting on a regular basis to senior management, the board, or a committee of the board, on compliance matters.
- Ensure appropriate compliance training to all staff by the Compliance Officer and Continuous Professional Development (CPD) hours required for the MLRO as per the FSC Competency Standards.
- Educating all staff with respect to compliance with the applicable laws, rules, and standards
- Establish good liaison with relevant external bodies, including regulators, standard setters, and external legal counsel.

The Compliance Officer reports directly to the Board and identifies, assesses, advises on, monitors, and reports on the company's compliance risk and thus assists Senior Management in discharging their compliance accountabilities. A detailed Annual Compliance Program is prepared and reviewed and submitted to the Board for their approval.

This manual has been designed taking into consideration the following:

- Financial Intelligence and Anti-Money Laundering Act 2002 (FIAMLA)
- Anti-Money Laundering and Combatting the Financing of Terrorism and Proliferation (Miscellaneous Provisions) Act 2019
- United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019
- AML/CFT Handbook 2020
- Prevention of Corruption Act 2002
- Prevention of Terrorism Act 2002
- Companies Act 2001
- Financial Services Act 2007
- Securities Act 2005
- Trusts Act 2001
- Rules and Regulations under the Financial Services Act 2007
- Regulations made under the Prevention of Terrorism Act 2002
- Regulations made under the Prevention of Corruption Act 2002
- Regulations under the Securities Act 2005
- Regulations under the FIAMLA 2002
- Codes and Guidelines as per the Financial Services Commission
- Anti-Money Laundering and Combating the Financing of Terrorism (AML/CTF) Framework
- Code of Business Conduct 2015

- Licensing Conditions of the Company as an Investment Dealer (Full-Service Dealer excl. Underwriting) License
- The Asset Recovery Act 2011
- FATF and other international standards and recommendations

COMPLIANCE OFFICER

Regulation 22 of the FIAML Regulations: "*…s.22(1)(a) designation of a compliance officer at senior management level to be responsible for the implementation and ongoing compliance of the reporting person with internal programmes, controls and procedures with the requirements of the FIAMLA and these regulations;*

…s.22(2) For the purpose of paragraph (1), the compliance officer shall have unrestricted access upon request to all books, records, and employees of the reporting person as necessary for the performance of his functions.
…s.22(3) The functions of the compliance officer designated under paragraph (1) shall include (a) ensuring continued compliance with the requirements of the FIAMLA and regulations subject to the ongoing oversight of the board of the reporting person 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 noncompliance, to the board and senior management; and
(d) contributing to designing, implementing and maintaining internal compliance manuals, policies, procedures and systems for combating money laundering and terrorism financing."

Functions Effected by The Compliance Officer

- Due Diligence is performed prior to accepting new clients.
- Ongoing periodic review of existing clients.
- Ensure that all policies, guidelines, procedures, and circulars are properly followed by all staff.
- Ensure timely submission of returns to the Regulatory Bodies.
- Inquire on complaints received from clients and report to Management.
- Submit periodical reports to Management for their immediate review and subsequent discussions and final comments.
- Annual review of the Compliance Manual.

MONEY LAUNDERING REPORTING OFFICER

The Company to appoint a Money Laundering Reporting Officer ("MLRO") and a Deputy MLRO in order to exercise the functions of the MLRO in his/ her absence. The DMLRO is of similar status and experience as the MLRO. Where this Manual refers to the MLRO it implies the DMLRO in the MLRO's absence.

The MLRO appointed by the Company must:

a) be a natural person;
b) be an approved officer under Section 24 of the FSA; and
c) have the appropriate knowledge, skill and experience in accordance with the Competency Standards issued by the FSC in October 2014;

The Company shall ensure that the MLRO:

a) is the main point of contact with the FIU in the handling of disclosures;
b) has unrestricted access to the CDD information of the Company's customers, including the beneficial owners thereof;
c) has sufficient resources to perform his or her duties;
d) is available on a day-to-day basis;
e) reports directly to, and has regular contact with, the Board or equivalent of the Company; and
f) is fully aware of both his or her personal obligations and those of the Company under FIAMLA and FIAML Regulations and the Handbook.

The main duties of the MLRO (as per the FSC Handbook) are at a minimum consist of the following:

- implementing and monitoring the day-to-day operation of the AML/CFT policy and procedures.
- reporting to the Board of Directors or a committee of the Board on any material breaches of the internal AML/CFT policy and procedures and of the AML/CFT laws, codes, and standards of good practice.
- preparing reports annually and such other periodic reports as he/she deems necessary to the Board of the Company or a committee of the Board dealing with: -
  - the adequacy/shortcomings of internal controls and other AML/CFT procedures implemented,
  - recommendations to remedy the deficiencies identified above,
  - the number of internal reports made by staff,
  - the number of reports made to the FIU.

ONGOING MONITORING

The frequencies for client files review are as follows:

1. "Low Risk" client
   A review of the client file should be carried out at least once a year.

2. "Medium Risk" client
   A review of the client file should be carried out every 9 months.

3. "High Risk" client
   A review of the client file should be carried out every 6 months.

Whenever a client is classified as "High Risk", his/her/its file must be forwarded to the Compliance Officer, which will analyse the case and take any additional actions deemed appropriate in line with the increased risk presented by the client, duly documenting its analysis in writing in the File Review Checklist.

Client Due Diligence (CDD) and Know Your Customer (KYC)

The most crucial step before starting any client, business and employee relationship is the process of Client Due Diligence ("CDD") which begins with Know Your Customer ("KYC") principles.

As a matter of internal policy, the full range of CDD measures should be applicable using a Risk-Based Approach as provided for in our Risk Profiling Checklist. CDD measures include:

- Identifying and verifying the identity of the applicant for business using reliable, independent source documents, data or information;
- Identifying and verifying the identity of the beneficial owner (ultimate owner), such that the Company is satisfied that it knows who the beneficial owner is.
- Obtaining information on the purpose and intended nature of the business relationship; and
- Conducting ongoing due diligence on the business relationship and scrutiny of transactions throughout the course of the business relationship to ensure that the transactions in which the client is engaged are consistent with the Company's knowledge of the client and his business and risk profile (including the source of funds).

AML/CFT Principle

The Company is required at the time of establishing a business relationship with an Applicant for Business and on an ongoing basis, using a risk-based approach apply appropriate Customer Due Diligence measures on the business relationship, including identifying and verifying the identity of the Applicant for Business.

The Company must undertake CDD measures and be satisfied of the results obtained. In cases of one-off transactions or a series of occasional transactions where the total amount of the transactions which is payable by or to the applicant for business is above 500,000 rupees or an equivalent amount in foreign currency, or whenever there is a suspicion of money laundering or terrorist financing at any point in time since the inception till the termination of the business relationship.

ENHANCED DUE DILIGENCE

Enhanced due diligence, as per Chapter 6 of the Handbook, would imply taking additional steps in relation to identification and verification. This may include the following steps:

- obtaining further client due diligence information (identification and relationship information) from either the client or independent sources (such as the internet, public or commercially available databases);
- verifying additional aspects of the client due diligence information obtained;
- obtaining additional information required to understand the purpose and intended nature of such a business relationship;
- taking appropriate and reasonable measures to establish the source of the funds and the wealth of the client, any beneficial owner and underlying principal; and carrying out more frequent and more extensive ongoing monitoring on such business relationships with setting lower monitoring thresholds for transactions connected with such business relationships.

The Company is required to carry out EDD in case of:

1. PEP
2. High Risk Jurisdiction

Client Identification Procedure

Identifying the Client

Identification and Verification of Applicants for Business who are Natural Persons.

Identification Data for Natural Persons

The Company must collect relevant identification data on a natural person, which includes:

- Name (including any former names, any other names used and other aliases)
- Current residential address
- Date and place of birth
- Nationality
- Any occupation, public position held and where appropriate the name of the employer

Verification of Identity of Natural Persons

(a) Verification of the identity of the natural person

The following types of identity documentation can be relied upon:

- National Identity cards
- Current valid passports
- Current valid driving licenses

(b) Verification of the address of the natural person

The following identity documentation can be relied upon to verify the address of the applicant for business if he/she is a natural person:

- A recent utility bill issued;
- A recent bank or credit card statement dated; or
- A recent bank reference.

N.B. 'recent' means within the last three months.

Alternatively, verification may be achieved by:

- Obtaining a reference from a professional person who knows the natural person. The reference must include the permanent residential address of the individual;
- Checking a current register of electors;
- Utilizing an address verification service; or
- Visit the individual at his/her current residential address.

Identification and Verification of Applicants for Business who are Legal Persons/ Arrangements

Legal Persons

Legal persons include bodies corporate, partnerships, associations or any other body of persons other than legal arrangements.

Verification of the Existence of a Legal Person and Identifying the Principals Thereof

Where an applicant for business is a legal person, the Company must –

- take reasonable measures to understand the ownership and control structure of the applicant for business;
- verify and establish the existence of the legal person; and
- determine the identity of the principals of the legal person.

For avoidance of doubt, in the case of a legal person, principals of applicants for business include the following:

- Promoters
- Beneficial owners and ultimate beneficial owners
- Officers
- Controllers
- Company Directors

The Company must:

- identify and verify the identity of the legal person, including name, incorporation number, date and country of incorporation or registration;
- identify and verify any registered office address and principal place of business (where different from the registered office);
- verify the legal status of the legal person;
- identify and verify the identity of underlying principal (including beneficial owners, controllers, directors or equivalent) with ultimate effective control over the capital or assets of the legal person; and
- verify that any person who purports to act on behalf of the legal person is duly authorized and identify that person.

Where the underlying principals are not natural persons, the Company must 'drill down' to establish the identity of the natural persons ultimately owning or controlling the business.

Private Companies

- Obtaining an original or appropriately certified copy of the certificate of incorporation or registration;
- Checking with the respective law firm/ registered agent that the company continues to exist;
- Obtaining a copy of the latest financial accounts, if available (audited, where possible);
- Obtaining a copy of the certificate of good standing;
- Obtaining details of the registered office and place of business;
- Verifying the identity of the principals of the company as above.

Legal Arrangements

Trusts do not have separate legal personality and therefore form business relationships through their business. It is the trustee of the trust who will enter into a business relationship on behalf of the trust and should be considered along with the trust as the client.

Verification of the Existence of a Legal Arrangement and Identifying the Principals Thereof

Where an applicant for business is a legal arrangement, the Company must –

- take reasonable measures to understand the ownership and control structure of the applicant for business;
- verify and establish the existence of the legal arrangement; and
- determine the identity of the principals of the legal arrangement.

For avoidance of doubt, in the case of a legal arrangement, principals of applicants for business include the following:

- Settlors or Contributors of capital (whether named or otherwise)
- Trustees
- Beneficiaries
- Protectors
- Enforcers

The Company must:

1. verify the legal status of the legal arrangement;
2. identify and verify the identity of the principals of the applicant for business, that is, those natural persons with a controlling interest and those who comprise the mind and management of the legal arrangement; and
3. obtain information concerning the name of trustee(s), its legal form, address and provisions binding the legal arrangement.

In relation to a trust, the above requirements can be achieved by:

1. Obtaining an original or appropriately certified copy of the trust deed or pertinent extracts thereof;
2. Where the trust is registered – checking with the respective trustee to ensure that the trust does exist;
3. Obtaining details of the registered office and place of business of the trustee;
4. Verifying the identity of the principals of the trustee as above.

Regulation 3 of the FIAML Regulations 2018 states that:

"3. (1) A reporting person shall —

a) identify his customer whether permanent or occasional and verify the identity of his customer using reliable, independent source documents, data or information, including, where available, electronic identification means, or any other secure, remote or electronic identification process as may be specified by the relevant regulatory body or supervisory authority;

b) verify that any person purporting to act on behalf of a customer is so authorised, and shall identify and verify the identity of that person;

c) identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using relevant information or data obtained from a reliable source such that the reporting person is satisfied that he knows who the beneficial owner is;

d) understand and obtain adequate and relevant information on the purpose and intended nature of a business relationship or occasional transaction;

e) conduct ongoing monitoring of a business relationship, including —

i. scrutiny of transactions undertaken throughout the course of the relationship, including, where necessary, the source of funds, to ensure that the transactions are consistent with his

knowledge of the customer and the business and risk profile of the customer;

ii. ensuring that documents data or information collected under the Customer Due Diligence (CDD) process are kept up to date and relevant by undertaking reviews of existing records, in particular for higher risk categories of customers.

2) Subject to paragraph (3), where there is a suspicion of money laundering, terrorism financing or proliferation financing, the reporting person shall, notwithstanding any applicable thresholds, undertake CDD measures in accordance with this regulation.

3) Where a reporting person suspects money laundering, terrorism financing or proliferation financing, and he reasonably believes that performing the CDD process, may tip-off the customer, he shall not pursue the CDD process and shall file a suspicious transaction report under section 14 of the Act.

4) A suspicious transaction report under paragraph (3) shall specify the reasons for not pursuing the CDD process

Regulation 4 of the FIAML Regulations 2018 states that:

"4(1) For a customer who is a natural person, a reporting person shall obtain and verify —

(a) the full legal and any other names, including, marital name, former legal name or alias;
(b) the date and place of birth;
(c) the nationality;
(d) the current and permanent address; and
(e) such other information as may be specified by a relevant supervisory authority or regulatory body.

4(2) For the purposes of paragraph (1), documentary evidence as may be specified by a relevant regulatory body or supervisory authority shall be used for the purposes of verification of identity requirement."

Regulation 5(1) of the FIAML Regulations 2018:

5. (1) Where the customer is a legal person or legal arrangement, a reporting person shall —

(a) with respect to the customer, understand and document —
(i) the nature of his business; and
(ii) his ownership and control structure;

(b) identify the customer and verify his identity by obtaining the following information —
i. name, legal form and proof of existence;
ii. powers that regulate and bind the customer;
iii. names of the relevant persons having a senior management position in the legal person or arrangement; and
iv. the address of the registered office and, if different, a principal place of business.

Regulation 6 of the FIAML Regulations 2018 states that:

6.(1) Where the customer is a legal person, the reporting person shall identify and take reasonable measures to verify the identity of beneficial owners by obtaining information on

a) the identity of all the natural persons who ultimately have a controlling ownership interest in the legal person;
b) where there is doubt under subparagraph (a) as to whether the person with the controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interests, the identity of the natural person exercising control of the legal person through other means as may be specified by relevant regulatory body or supervisory authority; and
c) where no natural person is identified under subparagraph (a) or (b), the identity of the natural person who holds the position of senior managing official.

(2) A reporting person shall keep records of the actions taken under paragraph (I) as well as any difficulties encountered during the verification process.

The Companies Act 2001 and the Financial Services Act 2017 prescribe a period of seven years.

Regulation 10 of FIAML Regulation 2018 states as follows:

In determining when to take CDD measures in relation to existing customers, a reporting person shall take into account, among other things —

(a) any indication that the identity of the customer or the beneficial owner, has changed;
(b) any transactions which are not reasonably consistent with his knowledge of the customer;
(c) any change in the purpose or intended nature of his relationship with the customer;
(d) any other matter which might affect his assessment of the money laundering, terrorist financing or proliferation financing risk in relation to the customer.

Regulation 11 of FIAML Regulation 2018 states as follows:

(1) Notwithstanding regulations 4, 5 and 6, a reporting person may apply simplified CDD measures where lower risks have been identified and the simplified CDD measures shall be commensurate with the lower risk factors and in accordance with any guidelines issued by a regulatory body or supervisory authority.

(3) Simplified CDD shall not apply where, a reporting person knows, suspects, or has reasonable grounds for knowing or suspecting that a customer or an applicant for business is engaged in money laundering or terrorism financing or that the transaction being conducted by the customer or applicant for business is being carried out on behalf of another person engaged in money laundering or terrorist financing.

Regulation 12 of FIAML Regulation 2018 states as follows:

(1) A reporting person shall perform enhanced CDD —

(a) where a higher risk of money laundering or terrorist financing has been identified;
(b) where through supervisory guidance a high risk of money laundering or terrorist financing has been identified;

(c) where a customer or an applicant for business is from a high risk third country;
(d) in relation to correspondent banking relationships, pursuant to regulation 16;
(e) subject to regulation 15, where the customer or the applicant for business is a political exposed person;
(f) where a reporting person discovers that a customer has provided false or stolen identification documentation or information and the reporting person proposes to continue to deal with that customer;
(g) in the event of any unusual or suspicious activity.

Measures applicable in case the Company is unable to conduct CDD measures.

Regulation 12(3) of the FIAML Regulations states that "…where a reporting person is unable to perform enhanced CDD where required under these regulations, he shall terminate the business relationship and shall file a suspicious transaction report under s.14 of the FIAMLA."

Third Party Reliance

The Company does rely on third parties for carrying out the CDD process and the Company shall be required to conduct a risk assessment on its third-party service providers.

CLIENT SCREENING

The Company is required to perform screening (e.g., World Check, Google Alert, Independent Google searches, OFAC, UNSC Consolidated List (National Sanctions Secretariat of Mauritius) and instantly against regular publications of the Financial Intelligence Unit Mauritius against its clients' name, and in case of entities, against the names of the beneficial owners, controllers, beneficiaries etc.

When conducting searches against the name of an individual or entity, the Company is required to consider "negative press" in addition to whether the individual or entity is named on a sanctions or PEP list.

Consideration should be given to the credibility of the information source, the severity of the negative press, how recent the information is and the potential impact the negative press would have on the business relationship with that customer.

As per Chapter 9 (s. 9.11) of the Handbook, the Company is expected by the FSC to document:

- the source and date of the search;
- actions taken to confirm or discount any potential match;
- details of the negative press;
- any actions taken to verify or disprove the claims; and
- any additional actions taken as a result of this information such as treating the customer as high risk and/or seeking proof of source of wealth/funds etc.

RISK ASSESSMENT FRAMEWORK

Introduction

This Risk Assessment Framework has been prepared in line with the Financial Intelligence and Anti-Money Laundering Act 2002 ('FIAMLA'), Financial Intelligence and Anti-Money Laundering Regulations

2018 (the 'FIAML Regulations'), the Anti-Money Laundering and Countering the Financing of Terrorism Handbook (the "Handbook") and the National Money Laundering and Terrorist Financing Risk Assessment of Mauritius Report 2019.

Purpose

A key component of the Risk Based Approach requires the Company to identify 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.

Framework

- The management and control of the ever-evolving risks and compliance culture are under the board of directors' ultimate responsibility.
- While performing business, the responsibility for the conduct of the BRA exercise must be shared by the Management, Compliance and Risk Management.
- The BRA should be conducted at least on an annual basis and on trigger events* and would be reviewed based on the Company's evolving size, nature, context, complexity and internal risk assessment.
- Risks, risks identification and mitigation exercises should be constantly reviewed and adapt to fit the emerging risks and the Company's reality.
- Periodic reports (at least annually) about AML/CFT Risk should be presented to the Board.
- The Company should appoint an AML/CFT Independent Auditor and conduct an AML/CFT Independent Audit in line with the Chapter 13 of the Handbook and Regulation 22(1)(d) of the FIAML Regulations 2018.

ML/TF Risk Assessment Process

The Company must, under Section 17(1) of the FIAMLA identify, assess, understand, and monitor its clients' ML and TF risks. The risk assessments involve making a judgement of a number of elements including threat, vulnerability, and consequence.

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

The Company has identified the following risk areas:

- The nature, scale, and complexity of the Company's activities.
- The products and services provided by the Company.
- The persons to whom and the manner in which the products and services are provided.
- The nature, scale, complexity, and geographical location of the customer and the customer's business activities.
- The delivery channels by which the Company provides its products and services.
- Reliance on third parties for elements of the CDD process.
- Technological developments.

Risk Control Measures

Risk

Risk can be seen as a function of three factors and ideally, a risk assessment involves making judgments about all three of these elements:

1. Threat - person or group of people, an object or an activity with the potential to cause harm. The threats may vary across customers, countries, geographic areas, products/services and delivery channels.
2. Vulnerability - that which can be exploited by the threat or that may support or facilitate its activities, such as size and volume of the business and client base profile.
3. Consequence - the impact or harm that ML or TF may cause, such as the impact on reputation and imposition of regulatory sanctions.

Action Plan of Risk Management Control and Mitigation

In the face of inherent ML/TF risks in each risk factors category, the Company, in line with the requirements of the FIAMLA, FIAML Regulations and the Handbook, and in considering the Company's nature of business and profile of its customer, adopts the following AML/CFT controls to mitigate the inherent risks which have been identified:

1. Appointment of a Compliance Officer and Money Laundering Reporting Officer at the senior management level to take charge of AML/CFT compliance matters
2. Proper policies and procedures
3. Ongoing training plan for directors and employees
4. Conduct risk assessment as per framework
5. Verification of customer identity and Customer Due Diligence
6. Screening for Targeted Financial Sanctions
7. Screening procedures to screen persons before recruitment
8. Enhanced due diligence measures
9. No cash transaction above MUR 500,000 or its equivalent in foreign currency
10. Application of dual control and the 4-eyes principles
11. Record keeping
12. Reporting of suspicious activities and/or transactions to the FIU
13. Regular review of internal controls, policies and procedures implemented

**Trigger Event is generally a transaction monitoring alert; in other circumstances it may include an adverse media alert or a law enforcement referral. Any major disruption to the financial market (e.g., pandemic, terrorist attack, etc.)*

Risk Factors and Risk Matrix

The Company analysed the ML/TF risks facing the Company in the risk factors category, with percentage weighting assigned as follows:

No.	**Risk Factors**	**% Weight Assigned**
1.	Nature, Scale, and Complexity of the Company's Activities	10%
2.	Product & Services Risk	20%
3.	Customer Risk	40%
4.	Delivery Channel	10%
5.	Third Party Reliance	10%

6.	Technological Risk	10%

Business Risk Assessment Sheet and Frequency

The Company should make an initial assessment using the Business Risk Assessment Sheet (Self-Assessment) and should be reviewed at regular intervals as outlined in the framework.

The Business Risk Assessment Sheet should be tabled at the Board meeting for ratification/ approval.

Client Risk Profiling and Classifications

Client Profiling

The Company has designed a client profiling document taking into account the Business Risk Assessment *(for Client)* and Client Risk Assessment.

Business Risk Assessment *(for Client)*

The Company should consider the extent of its exposure to risk by reference to a number of factors, such as operational risk, systemic risk, reputational risk, legal risk, complexity of any given structure, jurisdiction of the business activities, amongst others. The examples provided in this Manual are not exhaustive and other factors may need to be considered depending on the nature of the business and its activities.

A key component of the Risk Based Approach requires the Company to identify 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 the Company's policies, procedures, and controls are proportionate and targeted appropriately.

S.17(2) of the FIAMLA requires the Company to assess 6 key areas when undertaking the business risk assessment amongst other risk factors:

1. The nature, scale, and complexity of the Company's activities
2. The products and services provided by the Company
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 CDD process
6. Technological developments

Client Risk Assessment

After the collection of the CDD documentation, the Company must make an initial assessment of the risk to which the business relationship will expose it and evaluate the client accordingly. In this exercise, the Company will take into consideration a number of factors, including but not limited to the following:

1. The nature and type of client
2. The commercial rationale for the relationship
3. The geographical location of the client's residence
4. The geographical location of the client's business interests and/or assets
5. The nature and value of the assets concerned in the relationship
6. The client's source of funds and where necessary the source of wealth

The Company must routinely consider the risks that all relationships pose to them and the manner in which those risks can be limited. To do so, the Company must be able to demonstrate the effective use of documented CDD information. If the Company does not 'know a client', it will not be in a position to recognize and manage the risks inherent to the relationship.

While a risk assessment should always be performed prior to entering a business relationship, for some clients, a comprehensive risk profile may only become evident once the client has begun transacting through an account. Therefore, on-going monitoring of client transactions and on-going reviews are fundamental components of an appropriate risk-based assessment. The Company may also have to adjust its risk assessment of a particular client based upon information received after the establishment of the relationship.

Risk Factors

Business Risk Assessment *(for Client)*	**Client Risk Assessment**
Mode of Contact	KYC Documents
UBO Identification	Source of Fund
Type of Client	Source of Wealth
Maturity of Business	Jurisdictions of Source of Fund/ Wealth
Country of Activities	Country of Residence/ Incorporation of Investor
Business Activities	PEP Status
Mode of Transaction	Screening
Reputational Risk	Relationship
	Product Types being subscribe to

The Company must, under s.17(1) of the FIAMLA identify, assess, understand, and monitor its clients' ML and TF risks. The risk assessments involve making a judgement of a number of elements including threat, vulnerability, and consequence.

Client Classification

For the purpose of AML/ CTF monitoring, clients will be classified as per following:

Low Risk

1. Individual and corporations with a normal course of business/ profession

Medium Risk

1. Farming
2. Agricultural activities
3. Hunting and other related gaming activities
4. Fish farming
5. Food processing

6. Textile and related manufacturing activities including leather footwear, etc.
7. Wood manufacturing and product thereof including pulp and paper

High Risk

1. Activities related to so-called "windfall revenue" incl. large amounts of foreign aid
2. Arms
3. Betting and Gambling
4. Business activities likely to cause Environmental Damage
5. Business involving PEP/ Military figures
6. Jewellery and precious stones
7. Cash intensive businesses incl. Foreign Exchange
8. Government/ Public Procurement Activities
9. Human Health Activities: Provision of health services, pharmaceutical products, and medical devices, incl. research, development, dispensing and promotion of same
10. Investment Advisory/ Asset Management Services
11. Live Animal Testing
12. New or Innovative Type of Business
13. Non-Licenced Asset Management Activities
14. Non-Licenced Financial Services Business
15. Privatisation: Buying or obtaining from government something of large economic value through the process of privatisation
16. Supra-National Organisations
17. Unlicensed Mobile Phones

Due Diligence Prior to Accepting Business Partners

The Company before getting into an agreement with business partners, will have to ascertain that they are duly licensed by a regulatory authority and are on the official public register. Business partners will include but not limited to Trustees/ Lawyers/ Management Companies/ Custodian Banks.

Section 17F of the FIAMLA – Record Keeping

s.17F (1) “A reporting person shall maintain all books and records with respect to his customers and transactions in accordance with subsection (2) and shall ensure that such records and books are kept for such time as specified in, and in accordance with, subsection (2).”

All transactional records must be retained for the duration of the client relationship and for a period of at least 7 years after the completion of the transaction to which it relates.

Know Your Employee

As crucial as it is to Know Your Customer, knowing your employee has an equal importance for all financial businesses. As part of our due diligence on potential employees, apart from name and address document, professional references/ previous employer records/ certificates of character where applicable will be sought from all potential employees. Employees will also have to sign a secrecy clause within the employment contract which will clearly state their engagement in not revealing the clients / business partners to any unrelated party whether in the course of employment or after leaving the Company.

Employee Compliance Check Requirements

The Company is required, under Regulation 22(1)(b) of FIAML Regulations, to implement programmes for screening procedures so that high standards are maintained when hiring employees.

In order to ensure that employees are of the required standard of competence, which will depend on the role of the employee, the Company must give consideration to the following prior to, or at the time of, recruitment:

a) obtaining and confirming details of employment history, qualifications and professional memberships;
b) obtaining and confirming appropriate references;
c) obtaining and confirming details of any regulatory action or action by a professional body taken against the prospective employee;
d) obtaining and confirming details of any criminal convictions, including the provision of a check of the prospective employee's criminal record; and
e) screening the employees against the UN's list of designated persons under terrorist and proliferation financing targeted financial sanctions.

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

COMPLIANCE POLICIES

RECORD KEEPING POLICY

The Company keeps all records in relation to its activities as required by the law. Records comprise of full and true written details of every transaction that the company conducts:

The records are kept:

- In physical form or electronic data storage in the computers' hard disc;
- For a period of at least 7 years after the completion of the transaction to which it relates;
- At the principal office of the Company or such other place as may be agreed; and
- For identification purposes as per the index of each file.

Pursuant to section 17(b) of FIAMLA 2002, the Company must keep such records, registers and documents as prescribed in Regulation 21(2) of the FIAMLA Regulations 2018. Furthermore section 29 of the Financial Services Act 2007 requires the Company to keep and maintain internal records of the identity of each Customer as well as full and true written records of all transactions relating to his business activities.

The Company is also required to maintain the following records on the suspicious reports being filed:

- The internal suspicion reports received by the MLRO;
- Records of action taken under the internal and external reporting requirements;
- When the MLRO has considered information or other material concerning the reports, but has not made a disclosure of suspicion to the FIU, a record of the information or material that was considered and the reason for the decision; and
- All reports made by the MLRO to the FIU.

PEP POLICY

PEPs are individuals who are or who have been entrusted with prominent public functions foreign, domestic, and international organisation PEP, as well as the close relatives and associates of such persons. *(Refer to the definition section of the FIAML Regulations)*

Business relationships with PEPs, family members or close associates of PEPs are deemed to pose a greater risk and therefore an Enhanced Due Diligence ("EDD") is required on a regular basis.

The nature of the parties concerned in PEP scandals attracts worldwide media attention. Therefore, more attention to EDD monitoring on a regular basis is required by the Company.

Although in recent years' corruption has been closely associated with PEPs, it is not against the law or regulation to have a PEP as a customer, but it is expected by the regulation and law that the following is carried out:

- Enhanced Due Diligence ("EDD") and High-Risk Rating for PEP client.
- Regular updates of customer data to identify any change in the situation and/or emergence of opportunity risk.
- Greater scrutiny to the transactions.
- Approval of Senior Management/Board of Directors for client acceptance and transaction processing.

Therefore, careful planning is the best approach to reducing PEP risks within any business. In this context, the Company has planned the following procedures and processes to identify PEPs and to deal with additional risks that a PEP may pose:

(a) Identification of PEPs

- A screening is carried out on the client.
- Ensure that relevant information is sought from the applicant (PEP Declaration Form) as well as refer to publicly available information and use a reliable screening tool (e.g., World-Check) to identify and ascertain that a person is a PEP. The use of such external sources however should not be relied upon in isolation. While the use of google cannot be condoned as the most reliable method of investigation, in many cases it provides the gateway to more accurate and credible sources of information, which can be relied upon for identifying and verifying the identity of the parties to an entity and, if someone is identified as a PEP, analyze the extent to which he may be exposed to sensible factors such as corruption and bribery. All the evidence/ facts must be taken into consideration when categorizing an individual as a PEP.
- The risk associated with PEPs differs according to particularities of countries concerned. Please also consult the Transparency International Corruption Perceptions Index at http://www.transparency.org/ and assess the PEP accordingly.
- Identify when there is a relationship concerning a PEP. A PEP can be either a person or a person related to a body corporate.
- Assess the risk posed by the PEP using a risk-based approach in order to gauge the level of risk involved and to determine the degree of enhanced scrutiny required.

(b) Managing PEP Risks

- When a prospective client is found out to be a PEP following a screening carried out on him, the appropriate EDD measures must be applied prior to accepting such a relationship and throughout the business relationship.

Enhanced Due Diligence Measures

1. Signature on PEP Declaration Form
2. Risk Assessment must be carried out - Risk Rating the client as 'High-Risk'
3. Obtain Senior Management or Board's approval before on-boarding the Client
4. Details of that person must be recorded in the PEP Register maintained by the Legal & Compliance Department.

- Discuss the proposed business relationship with the Compliance Officer in light of information gathered on the PEP, including the source of fund and wealth and to obtain the written approval of Senior Management prior to establishing business relationship.
- Where a person is categorized as PEP or related to a body corporate in the course of a business relationship because of a change in his situation, discuss the change in the situation with the Compliance Officer and obtain written approval of Senior Management/Board of Directors of the Company to continue the business relationship.
- Obtain written approvals of Senior Management of the Company in cases of family members or close associates of PEPs.
- Conduct enhanced ongoing monitoring of the business relationships involving PEPs, family members or close associates of PEPs and of each business transaction.
- The Company will request an internal audit functions to consider PEP risk as an area for review.

TRANSACTION MONITORING POLICY

Transactions will be rated as either of these:

1. Low Risk

Transactions below a threshold of USD 12,500/- or its equivalent in another currency will be classified as Low Risk.

2. High Risk

Transactions amounting or exceeding a threshold of USD 12,500/- or its equivalent in another currency will be classified as High Risk.

Examples of High-Risk transactions include.

- Transactions involving large amounts (payments above USD 12,500/-)
- Transactions involving clients rated as 'High Risk' as per Risk Profiling Checklist
- Transactions involving PEP clients
- Transactions involving non-recurrent beneficiaries
- Transactions not in the ordinary course of business

- Transactions without business rationale
- Transactions where supporting documents are missing
- Transactions where transfer instructions and other communications were received from an email address different from that initially provided by the client.

PROCEDURE FOR PROCESSING A TRANSACTION

1. Understand the rationale of the transaction
2. Escalate to the reporting line should there be any doubt or suspicion on the payment
3. Ensure that approval of the Directors/ Senior Management is obtained where necessary*
4. Double click on the displayed sender's name to check if the email is genuine and corresponds with what the client has provided
5. Ensure that all relevant parties at the Company are copied on emails concerning the payment instruction
6. Tally the details sent by the client with the information on file (Check the business plan/ activity, investment details, names/ list of beneficiaries and their bank details, supporting documents like agreements, whether it is a new or recurrent payment, relevant resolutions, etc.)
7. Ensure that there are sufficient funds in the paying account
8. Ensure that the specimen signature for all bank signatories has been provided
9. Check the exchange rate and try to negotiate for the best rates
10. Prepare the wire transfer
11. Prepare all relevant documents (Invoice, agreement, resolutions, etc.) that need to be enclosed with the wire transfer
12. Call the client to confirm the transaction

** The circumstances are as follows:*

a) Where transaction involves clients categorised as PEPs.
b) For High-Risk clients, where transaction is above USD 12,500/-.
c) Where transaction involves any Officer of the Company.

ADDITIONAL PAYMENT PROCEDURE FOR HIGH-RISK TRANSACTIONS

- Conduct a screening or CDD on any non-recurrent beneficiary or third party to establish and verify identity
- Ensure all supporting documents such as agreements, resolutions, invoices, title deeds or any other relevant documents are obtained
- The Operation Manager must state, on the Approval Sheet, that he acknowledges that the transaction is 'High Risk' and that all due care has been taken when preparing payment.
- The bank signatories must state, on the Approval Sheet, that they are satisfied with the transaction and that they have checked the relevant supporting documents.

MONITORING OF CLIENTS ACTIVITY

The Company will maintain a transaction file for each client and the latter will be updated following each trade execution. Moreover, a file of all clients' transactions will be maintained, and a report analysis will be done every month to monitor the activity trend of all clients in line with AML/ CFTP requirements.

2. AML/ CFT MANUAL

Money Laundering

Money laundering is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities. If undertaken successfully, it allows them to maintain control over those proceeds and, ultimately provides them with a legitimate cover for the source of their income.

It is vital in the fight against crime that criminals be prevented, whenever possible, from legitimizing the proceeds of their criminal activities by converting funds from 'dirty' to 'clean'.

Reference is made to s.3(1) of the FIAMLA:

s3(1) Any person who –
(a) engages in a transaction that involves property which is, or in whole or in part directly or indirectly represents, the proceeds of any crime; or
(b) receives, is in possession of, conceals, disguises, transfers, converts, disposes of, removes from or brings into Mauritius any property which is, or in whole or in part directly or indirectly represents, the proceeds of any crime, where he suspects or has reasonable grounds for suspecting that the property is derived or realized, in whole or in part, directly or indirectly from any crime, shall commit an offence.

The laundering process is generally accomplished in three stages, as follows, which may comprise numerous transactions by the launderers that could trigger suspicion on money laundering.

1) **Placement** - the physical disposal of the initial proceeds derived from illegal activity.

2) **Layering** - separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity.

3) **Integration** - the provision of apparent legitimacy to criminally derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as normal business funds.

The three basic steps may occur as separate and distinct phases. They may also occur simultaneously or, more commonly, they may overlap. How the basic steps are used depends on the available laundering mechanisms and the requirements of the criminals.

Terrorist Financing

The Company has to take reasonable steps through the internal controls to ensure that its services are not being used for criminal activities linked to terrorist financing.

Obligations of Financial Institutions

In order to combat money laundering and the financing of terrorism, every financial institution must take measures to ensure that neither it nor any services offered by it is capable of being used to commit or facilitate the commission of a money laundering and/ or terrorist financing offence.

Reference is made to s.3(2) of the FIAMLA:

S3(2) A reporting person who fails to take such measures as are reasonably necessary to ensure that neither he, nor any service offered by him, is capable of being used by a person to commit or to facilitate the commission of a money laundering offence or the financing of terrorism shall commit an offence.

In addition, financial institutions have, in terms of the FIAMLA, a duty to verify the true identity of the clients and other persons with whom they conduct transactions.

PROLIFERATION FINANCING

Legal Frameworks

The United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 and the Anti-Money Laundering and Combatting the Financing of Terrorism and Proliferation (Miscellaneous Provisions) Act 2019 were enacted on the 21 May 2019 and both acts came into operation on the 29 May 2019.

The United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 enables Mauritius to implement the measures under all the United Nations Security Council Resolutions and deal with other matters of international concern, and to give effect to Article 41 of the Charter of the United Nations.

What is Proliferation?

Proliferation refers to the development and use of nuclear, chemical, or biological weapons and their delivery systems – also referred to as weapons of mass destruction ("WMD") – by state or non-state actors in violation of international agreements and export control regimes.

In Mauritius, "proliferation" is defined under s.2 of the FIAMLA and means -

a. the manufacture, production, possession, acquisition, stockpiling, storage, development, transportation, sale, supply. transfer, export, transhipment or use of –
    i. nuclear weapons
    ii. chemical weapons
    iii. biological weapons
    iv. such materials, as may be prescribed, which are related to nuclear weapons, chemical weapons, or biological weapons; or
b. the provision of technical training, advice, service, brokering, or assistance related to any of the activities specified in paragraph (a).

What is the Financing of Proliferation of Weapons of Mass Destruction?

Proliferation of weapons of mass destruction ("WMDs") can be in many forms, but ultimately involves the transfer or export of technology, goods, software, services or expertise that can be used in programmes involving nuclear, biological or chemical weapons, and their delivery systems (such as long-range missiles).

Proliferation of WMD financing is an important element and, as with international criminal networks, proliferation support networks may use the international financial system to carry out transactions

and business deals. Unscrupulous persons may also take advantage of the potential profits to be made by facilitating the movements of sensitive materials, goods, technology, and expertise, providing seemingly legitimate front organisations, or acting as representatives or middlemen.

All staff of the Company should be adequately trained in ML, TF and PF including MLRO. The frequency of the training can be assessed based on the complexity of the nature of the business but should be at least once a year.

Targeted Financial Sanctions

Obligations

The UNSC has imposed sanctions to prevent and counter the proliferation of WMD, and its financing. This includes targeted financial sanctions against specific persons and entities that have been identified as being connected to the proliferation of WMD. All UN member states are required to implement these measures.

Recommendation 7 of the FATF Standards requires countries to implement proliferation-related targeted financial sanctions (TFS) made under UNSC Resolutions without delay.

FATF Recommendation 7

"Countries should implement targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. These resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations."

Reporting Obligations & Procedures

Sanctions Reports

If a true match is identified by a reporting person, it must immediately submit a report to the National Sanctions Secretariat, and in some cases also to its relevant supervisory authority.

Reports may be completed using the template which can be downloaded from the NSSec website:

Reports must be submitted to the following email address: nssec@govmu.org.

Understanding Sanctions Evasion

Common sanctions evasion techniques used by proliferators include:

1. The use of aliases and falsified documentation to hide involvement of listed party.
2. Bank accounts owned by nationals not from a proliferating country, who act as financial representatives on behalf of listed parties from the proliferating country.
3. Offshore, front and shell companies to hide beneficial ownership information, and the involvement of listed parties.
4. Listed parties entering joint ventures with non-listed companies.
5. Use of diplomatic staff bank accounts, on behalf of listed parties and proliferating countries.

6. Use of virtual currencies by listed parties to circumvent the formal financial system and evade sanctions.
7. Conduct cyber-attacks against financial institutions and crypto currency exchanges to raise funds and evade sanctions.

The United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 is the Company's primary sources of law in matters of Targeted Financial Sanctions.

Obligations under FIAMLA

The company's obligations under the above legislations include

1. Maintaining a record of prescribed transactions
2. Furnishing information of prescribed transactions to the specified authority
3. Verifying and maintaining records of the identity of its clients
4. Keeping records in respect of (1), (2) and (3) above for a period of seven years from the date of cessation of transactions with the customers
5. In addition, the company will take such measures as are reasonably necessary (through an effective internal control) to ensure that it will not be used by any person to commit or to facilitate the commission of money laundering and / or terrorist financing.

Why AML/ CTF Policy?

- To prevent criminal elements from using the Company for money laundering and / or terrorist financing activities.
- To enable the Company to know / understand the clients and their financial dealings better, which in turn would help to manage risks prudently.
- To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws and laid down procedures.
- To comply with applicable laws and regulatory guidelines.
- To take necessary steps to ensure that the relevant staff are adequately trained in KYC/AML procedures.

Role of the MLRO

- Responsible for implementing and monitoring the day-to-day operation of the Company's AML/CTF policy and procedures
- Monitoring of suspicious activity
- Receives Suspicious Transaction Reports (STRs) from other staff
- Formulates STRs
- Evaluates STRs received
- Conduct internal investigation for all STRs received
- Reports to the FIU when deemed necessary after evaluation
- Reports to the board of directors of the Company or a committee of the board on any material breaches of the internal AML/CTF policy and procedures and of the AML/CTF laws, codes and standards of good practice
- Prepares reports annually and such other periodic reports deemed necessary to the board:
    - on the adequacy/shortcomings of internal controls and other procedures implemented to combat Money Laundering (ML) and / or Terrorist Financing (TF)
    - recommendations to remedy the deficiencies identified above
    - the number of internal reports made by staff and

    - the number of reports made to the FIU
- Risk management linked to money laundering and terrorist financing
- Liaison to all regulatory authorities
- Ongoing and periodic training to all staff.

Regulation 25(1) of the FIAML Regulations 2018 states that:

A reporting person shall examine, as far as reasonably possible, the background and purpose of all transactions that —
(a) are complex transactions;
(b) are unusually large transactions:
(c) are conducted in an unusual pattern; or
(d) do not have an apparent economic or lawful purpose.
(2) Where the risks of money laundering or terrorism financing are higher, a reporting person shall conduct enhanced CDD measures consistent with the risk identified.

Regulation 26(1) of the FIAML Regulations 2018 states that:

26(1) A reporting person shall appoint a Money Laundering Reporting Officer to whom an internal report shall be made of any information or other matter which comes to the attention of any person handling a transaction and which, in the opinion of the person gives rise to knowledge or reasonable suspicion that another person is engaged in money laundering or the financing of terrorism.

A reporting person shall appoint a Deputy Money Laundering Reporting Officer to perform the duties of the Money Laundering Reporting Officer in his absence. (4) The Money Laundering Reporting Officer and the Deputy Money Laundering Reporting Officer shall

(a) be sufficiently senior in the organization of the reporting person or have sufficient experience and authority; and

(b) have a right of direct access to the board of directors of the reporting person and have sufficient time and resources to effectively discharge his functions.

REPORTING OBLIGATIONS & PROCEDURES

Every financial institution has a duty under the FIAMLA to forthwith make a report to the FIU of any transaction which the financial institution has reason to believe may be a suspicious transaction. Financial institutions are required to use the goAML platform of the FIU to report suspicious transactions.

The contact details of the FIU are as follows:

"The Director
Financial Intelligence Unit
7th Floor, Ebène Heights
34, Ebène Cybercity
Ebène
Republic of Mauritius
Tel: (230) 454 1423
Fax: (230) 466 2431
Email: fiu@fiumauritius.org"

SUSPICIOUS TRANSACTIONS

'Suspicious transaction' is defined under FIAMLA 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, terrorist financing, proliferation financing or by proscribed organizations, 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; (e) gives rise to suspicion for any other reason.

MONITORING OF TRANSACTIONS

The Company has systems in place to detect complex, unusual or suspicious transactions or patterns of activity for all accounts. It has also established and maintain adequate systems and processes to monitor transactions. The design, degree of automation and sophistication of transaction monitoring systems and processes have been developed appropriately having regard to the following factors:

- the size and complexity of its business;
- the ML/TF risks arising from its business;
- the nature of its systems and controls;
- the monitoring procedures that already exist to satisfy other business needs;
- the nature of services provided;
- the transaction is international in nature, does the clients have any obvious reason for conducting business with the other country involved;
- significant transactions (in terms of amount or volume) for that client;
- the transactions that exceed transaction or amount limits;
- the geographical origin/destination of a transaction (jurisdictions that pose a higher risk to their particular sector or client type;
- transactions made by clients which pose higher money laundering and terrorism financing risks, such as High Net Worth Individuals, Politically Exposed Persons amongst others;
- the transactions outside the regular pattern of an account's activity; and
- unusual flow of funds.

WHY DO WE HAVE SUSPICIOUS TRANSACTION PROCEDURES?

Not all unusual or suspicious transactions will be cases of money laundering or funds gained from illicit activity. However, there is a duty to report cases that are found to be "suspicious" and let the proper investigations be conducted.

It is extremely important for staff to understand what they are doing and to not merely do as they are told. Members of staff are requested to use a logical and common-sensical approach and always attempt to decipher the reason for a particular transaction or state of affairs. If something does not make sense or cannot be explained according to the surrounding circumstances of a particular business or transaction, then staff should forthwith notify the MLRO.

It is the duty of the employee under the law to make a report of any suspicious transaction that he/she comes across and where an employee makes a Suspicious Transaction Report ("STR") to the MLRO, he/she will have discharged his/her legal obligation to report under the FIAMLA 2002.

The STR should be remitted directly to the MLRO or the Deputy MLRO and not be compromised by any other staff within the Company. As soon as the MLRO receives the report, all details will be logged on the goAML platform.

All KYC details need to be rigorously screened and investigated by the MLRO and any other employee that might be more familiar with the client details to determine whether the STR has any foundation. All contributions and memos should be made in writing.

If the investigation can unequivocally be found to be without foundation, then the matter is closed, and the findings logged.

If there is any remaining suspicion, no matter how trivial, then a full report must be submitted to the FIU through the goAML platform, and the relevant details entered into the STR log.

DUTIES UNDER FIAMLA AND FIAML REGULATIONS 2018

Section 14(1) of the FIAMLA states that:

"[…] 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."

Section 17(1) of the FIAMLA states that:

(1) "Every reporting person shall –

a. take appropriate steps to identify, assess and understand the money laundering and terrorism financing risks for customers, countries or geographic areas and products, services, transactions or delivery channels; and

b. consider all relevant risk factors before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied".

(3) "Prior to the launch of a new product or business practice or the use of a new or developing technology, a reporting person or a supervisory authority shall identify and assess the money laundering or terrorism financing risks that may arise in relation to such new products or business practices, or new or developing technologies for both new and pre-existing products and take appropriate measures to manage and mitigate these risks."

(4) "Every reporting person shall document the risk assessments in writing, keep it up to date and, on request, make it available to relevant competent authorities without delay."

Regulation 22 of the FIAML Regulations 2018 states that:

"22. (1) Every reporting person shall implement programmes 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 the following internal policies, procedures, and controls —

(a) designation of a compliance officer at senior management level to be responsible for the implementation and ongoing compliance of the reporting person with internal programmes, controls and procedures with the requirements of the Act and these regulations;

(b) screening procedures to ensure high standards when hiring employees;
(c) an ongoing training programme for its directors, officers, and employees to maintain awareness of the laws and regulations relating to money laundering and terrorism financing to —
(i) assist them in recognizing transactions and actions that may be linked to money laundering or terrorism financing; and
(ii) instruct them in the procedures to be followed where any links have been identified under sub subparagraph (i);(...)"

(d) an independent audit function to review and verify compliance with and effectiveness of the measures taken in accordance with the Act and these regulations.

This Regulation should be read in conjunction with Chapter 12 of the FSC Handbook 2020.

IDENTIFYING A SUSPICIOUS TRANSACTION

Refer to the Guidance Note 4 issued by the Financial Intelligence Unit (FIU), in force with effect in November 2020 for information inter alia on how to identify a Suspicious Transaction.

This Guidance Note has been prepared pursuant to section 10(2)(c) of the FIAMLA and is intended, *inter alia*, to guide Money Laundering Reporting Officers (and their Deputies) in completing the Suspicious Transaction Report form issued by the FIU. It is provided as general information only and it is not intended to act as a substitute for your own assessment, based on your own judgement, knowledge as well as on the specific circumstances of the transaction.

INTERNAL PROCEDURE FOR THE REPORTING OF SUSPICIOUS TRANSACTIONS

Staff must report any suspicious transaction to the Money Laundering Reporting Officer ("MLRO") using the Internal Disclosure Form, in order to discharge their reporting legal obligations.

The MLRO of the Company will review the matter and evaluate the Internal Disclosure, after which a report to the Financial Intelligence Unit ("FIU") will be made – as and when required.

In the absence of the MLRO, any suspicious transaction should be reported to the Deputy MLRO of the Company on the Internal Disclosure Form.

The Legal & Compliance Department of the Company will maintain an Internal Suspicious Transaction Report ("STR") Register, in which all the internal suspicious transactions which have been reported to the MLRO/Deputy MLRO will be recorded.

DUE DILIGENCE

The Company must undertake CDD measures and be satisfied of the results obtained:

- In cases of one-off transactions or a series of occasional transactions where the total amount of the transactions which is payable by or to the applicant for business is above 500,000 Mauritian Rupees or an equivalent amount in foreign currency; or
- Whenever there is a suspicion of money laundering or terrorist financing at any point in time since the inception till the termination of the business relationship.

RECORD KEEPING

As per section 17F of the FIAMLA, all transactional records must be retained for the duration of the client relationship and for a period of at least seven years after the completion of the transaction to which it relates.

As per Chapter 11 of FSC Handbook 2020, transactional records will include records containing information in individual transactions as follows:

- name and address of the client, beneficial owner and underlying principal
- if a monetary transaction, the currency and amount of the transaction
- source and destination of funds including full remitter details (instructions, forms of authority)
- account name and number or other information by which it can be identified
- details of the counterparty, including account details
- sale and purchase agreements as well as service agreements
- nature of the transaction
- date of the transaction

Identity records should be maintained for the duration of each relationship and for a period of at least 7 years thereafter.

Records of all anti-money laundering training delivered to employees must also be maintained.

Records of internal Suspicious Transaction Reports (STRs) made and STRs filed with the FIU should be maintained for the duration of the client relationship and all records should be retained for a period of at least 7 years after the completion of the transaction.

Obligation to Report

As per section 17G of the FIAMLA, "A reporting person shall, within the prescribed time limit, submit a report to FIU in the prescribed manner of any currency transaction in an amount equal to or above the prescribed amount, whether conducted as a single transaction or several transactions that appear to be linked".

Upon a court order, the Company shall make available such records, registers and documents as may be required by the order.

Tipping Off

S.19(1)(c) of the FIAMLA provides for the offence of 'tipping off' - which offence is committed when a person, knowingly or without reasonable excuse, warns or informs the owner of any funds of any report or any action that is to be taken in respect of any transaction concerning such funds.

The FIAMLA expressly prohibits a person who is directly or indirectly involved in the reporting of a suspicious transaction from divulging to any person involved in the transaction or to any unauthorized third party with the exception of the Regulatory Body that the transaction has been reported. If a person is found guilty of 'tipping off' he may, on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

In practice, preliminary enquiries in respect of an applicant for business, either to obtain additional information to confirm true identity, or to ascertain the source of funds or the precise nature of the transaction being undertaken, will not trigger a 'tipping off' offence. Great care should, however, be taken where a suspicious transaction has already been reported and it becomes necessary to make further enquiries, to ensure that customers do not become aware that their names have been brought to the attention of the FIU.

Malicious reporting: If anyone submits an STR to the FIU without reasonable grounds or maliciously, the Company may be sued for breach of client confidentiality. However, if a disclosure is made in good faith but proves to be groundless, then the Company may claim immunity.

Failure to Report

Any financial institution or any director or employee thereof who knowingly or without reasonable excuse fails to lodge a report of a suspicious transaction, commits 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.

Sanctions

Where it appears to the Regulatory Body that any financial institution subject to its supervision has failed to comply with any requirement imposed by FIAMLA or any regulations applicable to that financial institution and that the failure is caused by a negligent act or omission or by a serious defect in the implementation of any such requirement, the FSC, in the absence of any reasonable excuse, may sanction the Company / individual as per the applicable laws.

TRAINING

Obligations

The Company is required, under Regulation 22(1)(c) of FIAML Regulations to carry ongoing training programmes for directors, officers and employees in order for them to maintain awareness of the laws and regulations relating to money laundering and terrorism financing and to (i) assist them in recognising transactions and actions that may be linked to money laundering or terrorism financing; and (ii) instruct them in the procedures to be followed where any links have been identified under sub subparagraph (i).

Training Requirements

As per Chapter 12 of the Handbook, all employees are made aware of the Company's Internal Control, Policies and Procedures. They are also informed of the identity of the MLRO and the Deputy MLRO as well as their responsibilities.

The Company would ensure that all its employees are appropriately trained and that the training programmes are designed in such a way that the following important aspects are covered:

- Legal obligations as well as aspects of the AML/CFT laws, regulations and guidelines;
- The money laundering and terrorism financing vulnerabilities of the products and services offered by the Company;
- The CDD requirements and the requirements for the internal and external reporting of suspicion;

- Recognition and handling of suspicious transactions/activities;
- The criminal sanctions in place for failing to report information;
- New developments including information on current money laundering and terrorist financing techniques, methods, trends and typologies; and
- Information on the changing behaviour and practices amongst money launderers and those financing terrorisms.

Employees would be provided with a minimum of at least one training session annually.

INDEPENDENT COMPLIANCE AUDIT POLICY

INTRODUCTION

The Independent AML/CFT Audit is as per the Chapter 13 of the Handbook, and as required under Regulation 22(1)(d) of the FIAML Regulations 2018. This Policy defines the principles and commitments of the Company regarding regulatory Compliance.

SCOPE OF INDEPENDENT AUDIT

The Independent Compliance Audit shall help to ascertain if the AML/CFT programme adopted by the Company throughout the specified period was adequate and effective and advises on any changes that may be required. This shall be done by testing compliance in the following non-exhaustive areas:

- AML/CFT Policies and Procedures
- Internal Risk Assessments
- Risk Assessments on the use of third-party service providers (Outsourcing)
- Compliance Officer functions and effectiveness
- MLRO/ Deputy MLRO functions and effectiveness
- Implementation and Effectiveness of Mitigating Controls, including Customer Due Diligence and enhanced measures
- AML/CFT Trainings
- Record Keeping Obligations
- Targeted Financial Sanctions
- Suspicious Transaction Monitoring and Reporting

AUDIT FREQUENCY

The Independent Compliance Audit shall be conducted on an annual basis and/or when there has been a major change in the AML/CFT risk assessment, policies, or procedures. However, the audit frequency shall be based on the internal risk assessment and any previous audits.

INDEPENDENCE OF THE AUDITOR

The Independent Compliance Audit shall be independent and separate from the operational and executive team dealing with the AML/CFT processes of the Company. An independent audit review will be conducted by an internal or external audit professional. Apart from being independent, the choice of the auditor should be based on the experience and skill of the latter. The background and qualifications of the auditor shall be asked prior to the audit. In order to ensure that the audit is properly conducted as required under the FIAMLA and FIAML Regulations 2018, the audit professional needs to provide quality recommendations, so that the Company can use the findings and recommendations to improve its internal process.

AUDIT REPORTING

Audit must be signed and cover results of reviews on above mentioned areas and shall be reported to senior management and the Company's Board of Directors.

FILING TO THE FSC

The Company shall file its independent audit report for a specified period, upon the request of the FSC.

INDEPENDENT AUDIT POLICY REVIEW

This policy will be reviewed annually or in the event of any changes in the law and/or any changes in our business practice.

3. CONFIDENTIALITY & SECURITY MANUAL

SECRECY OBLIGATION

All employees, advisors and committee members shall keep in mind that, basically, all information received from a client is confidential, except when the employee, advisor and committee member certify himself that the information is publicly available. In case of doubt, prior to disclosing, the employee, advisor and committee member shall check with Managing Director or the Board.

Confidential information shall only be disclosed to (i) employees, advisors and committee members of the Company who need access to it in order to perform their job; (ii) external attorneys, consultants and auditors; and (iii) participants in a possible transaction, provided that, this information is directly related to the transaction and is disclosed on a need-to-know basis. However, it is essential that the person to whom the information is disclosed expressly undertakes to maintain the confidentiality of such information.

All confidential information available in client's files shall not be used for any other purposes except those for which it is intended, neither may it be supplied to third parties who are not directly linked to the transaction, except when there is a written consent by the client.

All employees, advisors and committee members must be aware that they are responsible for the secrecy of confidential information obtained in the course of their functions. The employees shall deal carefully with such information, using their best efforts to advise third parties and work associates to keep the same secrecy.

In the event an employee, advisor and committee member have access to confidential information not directly related to his or her work, he or she shall immediately communicate this fact to the Board or a director.

Those responsible for controlling confidential information shall take the necessary security measures so as to avoid taking, distributing and keeping unnecessary copies. A special care shall be taken upon copying confidential information and keeping it at locations such as workstations, meeting rooms, etc.

Matters referring to confidential information shall not be discussed in public locations such as restaurants, elevators, toilets and similar places where there is a risk that such information may be disclosed.

With the objective of maintaining adequate control of confidentiality, an evaluation shall be made when delegating auxiliary functions involving the handling of confidential information to secretaries, office boys, temporary employees, etc.

CONFIDENTIAL INFORMATION

The unauthorized release of confidential information can cause the Company to lose critical competitive advantage, hurt relationships with clients and embarrass or harm fellow employees. Confidential information is any information or knowledge created, acquired or controlled by the Company that it has determined to safeguard from improper public disclosure. Confidential

information may include, but is not limited to, the Company's clients, databases, systems, marketing and strategic plans, financial records, and business plans.

In the course of carrying out the Company's business, employees, officers and directors of the Company often have access to confidential or proprietary information about the Company, its customers, suppliers, or other business partners that might be harmful to the relevant party or useful or helpful to competitors if disclosed. Therefore, all employees, officers and directors are required to maintain the confidentiality of information entrusted to them by the Company, its customers, suppliers, vendors or other business partners, except when disclosure of such information is authorized by the Company or legally required by a court of law or under the FIAMLA 2002 when the MLRO/ Deputy MLRO file an STR.

In order to avoid the inadvertent disclosure of confidential information, employees, officers and directors should refrain from discussing such information with or in the presence of any unauthorized persons, including family members and friends.

BUSINESS RECORDS AND COMMUNICATION

All staff members are responsible for the integrity of business records and communications that are created. Making false or misleading entries in the Company's books and records is strictly prohibited. All records - including marketing, sales, travel and entertainment, purchasing and finances must be accurate and complete.

If anyone is not certain as to the accuracy of information on the Company's record, he/she should ask about it. No one should by his/her silence, allow himself/herself to become responsible for an incorrect record.

PROTECTION AND PROPER USE OF THE COMPANY ASSETS

Company assets should be used efficiently and for legitimate business purposes only. Employees, officers and directors are personally responsible for protecting Company assets entrusted to them and for helping to protect the Company's assets in general.

OUTSIDE EMPLOYMENT

Employees should not engage in any form of business or employment, with or without compensation outside the Company unless prior approval has been obtained from the Board of Directors.

The Board should ensure that it does not accept employment or engage in activities which may conflict or interfere with the performance of its duties or cast doubts on its own integrity or that of the Company.

DISCLOSING INFORMATION

Timely, accurate, and complete disclosure of relevant information in an appropriate manner should be a commitment for all of the Company team members. The Company must meet the disclosure expectations of all its external stakeholders and the continuous disclosure obligations as per law and regulating bodies if relevant.

The Company will make all financial information filings required by law and ensure that annual and interim reports are in line with overall communication plan and vetted against strategic policy goals.

Moreover, the Company will ensure that selective disclosure of material information does not occur.

DUTY OF CONFIDENTIALY

The Company personnel have, as per law, the duty of confidentiality to the Company. The Company requires all its personnel to act in good faith and to avoid placing their own personal interests above those of the Company.

The Company is very sensitive to the issue of the protection of trade secrets and other confidential and proprietary information of both the Company and third parties. Therefore, employees are expected to use sound judgement and to adhere to the highest ethical standards when using or communicating 'Confidential Information' on the Company's technology resources.

'Confidential Information' should not be accessed through the Company's technology resources in the presence of unauthorised individuals. Similarly, 'Confidential Information' should not be left visible or unattended.

Any 'Confidential Information' transmitted via technology resources for example email facility should carry the following confidentiality disclaimer:

'The information in this email and any files attached are confidential and may be privileged. If you are not the intended recipient, please destroy this message, delete any copies held on your systems and notify the sender immediately. You should not retain, copy, use or disseminate this email for any purpose, nor disclose all or any part of its content to any other person.'

RELEASE OF INFORMATION

GUIDELINES FOR MATERIAL INFORMATION DISCLOSURE

When releasing material information, the Company will adhere to the following:

- When it is decided to disclose material information, this information must immediately be broadly disclosed to all relevant audiences via press releases;
- One must ensure that in this disclosure, no information is omitted that would make the rest of the disclosure misleading (i.e., no half-truths or inaccuracies that can be misleading);
- Unfavourable material information must be disclosed as immediately and completely as favourable information;
- Disclosure on the Company's website only should not be considered as adequate disclosure of material information;
- There should be no selective disclosure. In other words, confidential material information must not be disclosed to selected individuals (for example, in an interview with an analyst or in a conversation with a significant investor);
- If there has been a mistake in an earlier material disclosure, this must be corrected as soon as possible.

4. BUSINESS CONTINUITY & DISASTER RECOVERY MANUAL

BUSINESS CONTINUITY & DISASTER RECOVERY PLAN

OVERVIEW

This Business Continuity and Disaster Recovery Plan for the Company provides an outline of preventative controls in place that help to avert disruptions, as well as action plans to be used in the event of a service disruption that may impact client's service deadlines. The Business Continuity and Disaster Recovery Plan provides for effective alternative operational methods in the event of a disruption of service lasting more than a specified time period. The time period required for activation of this plan would be dependent on the affected operational areas and severity of the disruptive event.

The objectives of the Business Continuity and Disaster Recovery Plan are:

- To ensure continued service to the Company clients
- To ensure timely resumption of essential operations
- To safeguard processing mechanisms and critical records
- To limit financial losses to the Company and its clients
- To ensure the security of its clients' data

BUSINESS CONTINUITY VERSUS DISASTER RECOVERY

It is important to note for the purposes of this plan that business continuity and disaster recovery are not interchangeable. Business continuity refers to the means by which loss of business may be avoided. This includes procedures or products put in place to reduce the likelihood of service disruptions due to any foreseeable reason. The primary goal of business continuity is 'High Availability'. Disaster recovery on the other hand, is the plan of action to be taken when there is a disruption of service for any reason. It includes both short term and long-term processes to be implemented depending on the severity of the disruption. Disaster recovery's main goal is 'High Level of Recovery'.

The Company has taken significant precautions to ensure the continuity of critical operational areas in the event of a service disruption. The possible threats to business continuity include those listed above and natural disasters such as floods, fires, and cyclones, as well as intentional sabotage and technology-related disruptions. Any other event that prevents access to the physical facilities, communications, or data may also be considered a disaster or service disruption event.

The disaster recovery portion of this plan provides a schedule for alerting clients when normal processing is not possible. Integral internal operations and critical services have been identified to assure that alternate service and recovery procedures are in place to facilitate service to clients in the event of a service disruption. Annual testing of this Business Continuity and Disaster Recovery Plan would be performed to ensure that the plan is both functional and effective. Senior Management as well as the Managers of each operational area would be trained on the proper implementation of this plan.

BUSINESS IMPACT ANALYSIS

Any Business Continuity and Disaster Recovery Plan must begin with a thorough business impact analysis.

- What events might lead to a service disruption?
- What operational areas would most likely be affected?
- How do the Company mitigates the risk of a service disruption to those areas?

The business impact analysis examines those questions and is used to set forth a plan that may be used in the event of a business disruption.

FUNCTIONAL DEPARTMENTS

The main operational areas of the Company are:

- Operation
- Marketing
- Sales
- Finance
- HR/ Admin

All business areas share the same accounting and payroll function, which can be addressed across the organization.

BUSINESS CONTINUITY & DISASTER RECOVERY SCENARIOS FOR COMMON OCCURRENCES

The following scenarios of service disruptions address a broad array of events that could require activation of the Business Continuity and Disaster Recovery Plan. While not every scenario can be envisioned, certain events that have occurred to other organizations can serve as a guide. With that in mind, the most common scenarios that might cause a service disruption are:

- Electrical failure
- Communications failure
- Data corruption/software failure
- Hardware failure
- Physical destruction of the building (fire, wind, cyclone)
- Any event that precludes access to the building (strike, chemical spill, hostage situation, flu pandemic, etc.)

The first four scenarios represent business continuity planning. These events can be anticipated, planned for, and are more likely to occur than the last two (total destruction or loss of use). Total loss of access to the facility is very unlikely but requires a much greater level of planning for effective recovery. There may be other specific events not stated here, but this list encompasses the end result of a broad range of events that could lead to activation of the plan.

PANDEMICS

In the event of a major outbreak, the Company would have to follow guidelines as issued by the Government and staff would be advised/ required to work from home. Staff would be required to attend to clients' queries, liaise with third party service providers for clients or liaise with relevant authorities to attend to the clients' requests from home. The Company would make provisions for its

staff to be in possession of laptops and provide mobile connection to key personnel as required. The Company would ensure that select managers and staff would have the capability to connect to the network remotely via secured VPN whereby they would be able to work safely from home or even outside the country. The internal phone system can be transferred to cell or home phones; hence voice communications would still be functional if a segment of the staff has to be quarantined or is unable to report to the office.

Management would work with a dedicated team to produce procedures and training for staff on how to limit the transmission of viruses in general to others in the workplace. Through awareness and training, the impact and potential of this threat should be minimized.

OUTSOURCED SERVICES

Based on the Company's requirements to overview the IT requirements including hardware and software support services, The Company would:

1. Have its own IT department/ personnel; or
2. Appoint an independent IT Service Provider.

BUSINESS CONTINUITY PLAN FOR COMMON OCCURRENCES

ELECTRICAL

Due to the very nature of the Company's business, it stores sensitive data and an electrical or communications failure would have a very significant impact. Statistically these two failures happen on a more frequent basis than a catastrophic event such as total destruction of a facility. Since that is the case, it is important to note that steps have been made to mitigate these two events that are not necessarily detailed as part of a full Disaster Recovery Plan for a worst-case scenario.

Currently, the Company occupies rental office space and ensures that the building is equipped with electrical generators. This would thus minimize the possibility of hardware or software failure. It also allows the continuation of processing in the event of a short-term power failure with minimal disruption and as additional safeguard the Company also makes provision for a UPS attached to the server.

DATA COMMUNICATIONS

Since data communications are absolutely business critical and the main medium currently used for exchange of data is internet connection, the Company is required to take steps to reduce the impact of a data communications failure by having backup internet connection which would ensure increased network security and would allow for internet access in case of a disruption. Backup internet connections lessen the chance that a common occurrence such as an internet outage would significantly impact daily processing. It does not ensure that internet communications would always be available but mitigates the impact in the event of an outage.

VOICE COMMUNICATIONS

A failure of voice communications would make operations difficult but would not qualify as a disaster event as there are other means of communications. However, the Company should ensure that it has proper voice communication facility whether it be by fixed line, mobile or internet- based communications.

DATA BACKUPS

The Company attaches great importance to the privacy and the protection of data of its client's information entrusted to it. It protects the data in accordance with applicable laws and our data privacy policies. In addition, the Company maintains the appropriate technical and organizational measures to protect the data against unauthorized or unlawful processing and/ or against accidental loss, alteration, disclosure, or access, or accidental or unlawful destruction of or damage thereto.

The Company retains copies of all documentation in relation to Customer due diligence information (refer to Chapter 5 of the AML/ CFT Handbook 2020), Transactions (refer to Chapter 9 of the AML/ CFT Handbook 2020) and Internal and external suspicious reports (refer to Chapter 10 of the AML/ CFT Handbook 2020).

The Company has protocols, controls and relevant policies, procedures, and guidance to maintain these arrangements. The records consist of original hard copy documents as well as data or documents maintained electronically. In any event, the Company is in a position to retrieve records easily and quickly. The Company periodically review the ease of retrieval of, and condition of, paper and electronically retrievable records.

Data related disruptions have been mitigated through the use of:

- Daily physical backups on internal drive on the server; and
- Daily cloud back-ups; and
- Weekly physical backups on external drive which is kept with the Managing Director ("MD") or any other Senior Management.

In the event the server is affected due to some reasons, the MD or the assigned personnel with the help of the IT Team can make effective use of the backup stored on the external drive or retrieval of data may be carried out from the cloud storage.

CLIENT NOTIFICATION

The Company would ensure that in the event of a disaster or contingency, clients and stakeholders are notified as appropriate. Senior Management is responsible for initiating the notification process. Clients would be notified as soon as possible/ practical after a disaster event to update them on operational contingency plans. Senior Management would coordinate via email, telephone, or internet.

Notification to clients would include:

- Type of disaster
- Extent of damage
- Plans for recovery
- Anticipated time for resumption of services
- Special processing instructions

ESCALATION

In the event of a disaster, any staff facing a problem at work would have to report to his/ her immediate superior who in turn would escalate the matter to Senior Management immediately.

Senior Management would in turn inform the board of directors and would in parallel appoint a Task Force comprising of Operation Manager(s), Compliance Officer(s), Finance Officer(s) and the IT Team.

During the disaster period, staff would be called upon to work from home or an alternate location. This decision would subsequently be communicated to the regulators and to all clients.

The Task Force would have to work on a plan within a set deadline with respect to the resumption of work back to normality.

5. COMPLAINT HANDLING PROCEDURES

COMPLAINT HANDLING

The complaint management procedures for the handling of complaints received by the Company aim to establish, implement and maintain effective and transparent procedures for the reasonable and prompt handling of complaints or grievances received from current or potential clients and keep a record of each complaint or grievances and the measures taken for the complaint's resolution.

The Manual for handling client's complaints gathers all measures taken by the Company in order to solve potential inconveniences that might occur among the business relation.

PROCEDURES

Filing Complaints

The clients willing to submit a complaint are advised to complete a Complaint Form and to send it to the Company through the following means:

- By sending an e-mail with a brief explication of the subject of complaint.
- By sending the complaint via registered mail.
- By sending the complaint via fax.

Receiving Complaints

After receiving the complaint, the Compliance Department notifies by the end of the next working day the complainant that his inquiry was received and provide him/ her with the name and the contact details of the person who is handling the complaint received.

Any Complaint Form received by the Company will be assigned a protocol number and registered in the Company's Complaints' Register duly maintained by the Compliance Department. The compliant will be examined and resolved by the Compliance Department in cooperation with the Relationship Manager involved with the complaint. Depending on the nature and the possible claims arising thereof, a briefing or an opinion may be sought from the Legal Advisor of the Company.

Handling Complaints

The Compliance Department is responsible for handling customers complaints or grievances. Their duties include the effective and efficient handling of client's complaints or grievances so as to enable the Company to adopt and apply the required actions to fully protect the clients' and the Company's interests, acting independently and objectively and ensuring that corrective measures are introduced to prevent the repetition of the same complaints or grievances. In the cases where the complaint or grievance involves the Compliance Department it is to be handled by the Operations Manager.

In the Compliance Officer's absence, the Operations Manager shall be responsible for the implementation of the Company's Complaints Handling Procedures.

The Complaint Form

The Compliance Department records the complaint in the client's Complaint Form which includes the following information:

- details of the client that made the complaint;
- the service/department to which the complaint refers to;
- the details of the employee responsible for the service/s rendered to the client;
- the date of receipt and of registration of the complaint;
- the content of the complaint, in brief;
- the capital and the value of the financial instruments which belong to the client and are registered in his account;
- the magnitude of the damage which the client claims to have suffered or which can be presumed to have suffered on;
- the basis of the contents of the complaint;
- the date and, briefly the content of the Company's written response to the complaint lodged;
- a reference to any correspondence exchanged between the Company and the client.

Review

The Compliance Officer shall review carefully the details of each client's complaint. Once the Compliance Officer understands fully the nature of the client complaint, he/ she shall investigate and question the relevant Head of the Departments related to each client complaint and will:

- Solve the complaint by replying to the complainant and informing the Director regarding the decision or seek assistance by the Relationship Manager or the Director.

Solving Complaints

The Head of the relevant department shall take all necessary measures:

- investigate and question the relevant personnel of the Departments related to each complaint (if necessary),
- communicate with other Head of Departments/ employees if this is required for solving the complaint,
- call the specific client for a personal interview or discuss the matter over the phone, as appropriate to identify the nature of the complaint.

If necessary, the Compliance Officer will investigate the relevant Head of Departments related to each client complaint. Once the Compliance Officer and the Director thoroughly analyse the matter, the decision will be communicated to the complainant and/ or the person in charge of the client complaint. Where applicable the Board of Directors as well as the Legal Advisor of the Applicant shall also be informed.

Time Frame

According to the Company's policy, the complaints will be solved in maximum 7 working days.

In case, due to the nature of the complaint, more time is required for the complaint to be fully investigated and solved, the Head of the relevant department should inform the Compliance Officer.

The Compliance Department shall notify the complainant about the investigation running and to inform him/ her about the approximate time period until the final response is sent, is laid down, which cannot be longer than 30 days starting from the working day following the reception of the initial complaint or the reception of additional evidence provided.

The Compliance Officer should fully investigate the complaint/ grievance in coordination with the Head of the concerned department and if deem necessary with the Director and/or the Legal Advisor.

Records and Measures

The Company shall maintain effective and transparent procedures for the prompt handling of complaints or grievances received from clients. The Company shall keep a record of each complaint or grievance as well as the measures taken for the complaint's/ grievance's resolution.

The Compliance Department shall maintain all complaints, all relevant correspondence and documents related to complaints, for a minimum period of seven years.

One copy of the Complaint Form is archived in the client's file and another copy is kept in a separate file ("Complaint/ Grievance File").

At the end of each month the Director inspects the "Complaint/ Grievance File" and ensures that the Head of the Departments have taken all the required actions so as to prevent repetition of the same complaints/ grievances.

The Compliance Officer make sure that manuals are updated to address and prevent the drawbacks in the Company's procedures that may cause malpractices and respectively customer's complaints.

The Relationship Manager shall inform at least once a year the Board of Directors of all complaints/ grievances received.

6. CONFLICT OF INTEREST

CONFLICT OF INTEREST POLICY

How conflict arises?

It is acknowledged that the services of the Company to any of its clients will not be exclusive. In the event of any conflict of interest or potential conflict of interest in respect of any investment or transaction, the Company will make disclosure of the existence of such conflict or potential conflict to the client.

General Principles

Each director of the Company shall make full disclosure to the Board of any conflict of interest or potential conflict of interest.

Employees and others acting on the Company's behalf must be free from conflict of interest that could adversely influence their judgment, objectivity or loyalty to the Company in conducting the Company's business activities and assignments. The Company recognizes that employees may take part in legitimate financial, business, charitable and other activities outside their employment, but any potential conflict of interest raised by those activities must be disclosed promptly to the management of the Company.

The Company's management approval should therefore be requested for outside activities, financial interests or relationships that may pose a real or potential conflict of interest.

Employees and others acting on the Company's behalf must obtain necessary approvals before accepting any position as an officer or director of an outside concern.

Addressing conflicts of interest

In order to gain the confidence of the authorities as to its objectivity and impartiality, rules and procedures will be established by the Company to guarantee that:

- Conflicts of interest are treated in a lawful and ethical way;
- The Company acts honestly, fairly and professionally when providing its services; and
- The personal transactions of the persons working under contract for the Company:
    - do not infringe legal requirements and business ethics; and
    - do not lead to conflicts between their personal interests, those of the Company and the clients.
- In the conduct of their duties, directors and employees of the Company:
    - will arrange their private affairs in a manner that will prevent real, apparent or potential conflicts of interest from arising;
    - will not solicit or accept transfers of economic benefit;

- will not step out of their roles to assist other outside entities or third parties in their dealings where this would result in a preferential treatment to the latter;
- will not knowingly take advantage of, or benefit from, any information that is obtained in the course of their official duties;

The Company shall ensure that it takes regular operational walk-through review including a pro-active approach to monitoring its business activities and may include specific ad-hoc compliance monitoring, a conflict register and information barriers. In the event of any proven conflict of interest, the Company proposes to handle the same in the following manner:

- When a conflict of interest is shown to have occurred, an ad-hoc committee will be put in place to enquire on the potential conflict of interest in order to put an end to it;

- When a proven conflict of interest has been confirmed, an arbitration process is organized depending on the complexity of the conflict of interest, so as to resolve the matter quickly and avoid harming the interests of the clients;

- However, when the risk of harming the interests of the clients is inevitable, the Company will inform the client of the general nature and origin of such conflict of interest, before taking action on their behalf. Having been alerted allows the clients to make an informed decision regarding provision of the services being offered to them.

- A conflict-of-interest register is maintained by the compliance department detailing all conflicts of interest including:

  - all conflicts of interest notification;
  - any reported cases of failure to disclose;
  - disclosure by others, such as colleagues or clients;
  - assessment of the matter and how it was considered;
  - any action taken; and
  - any reviews of the assessment process.

- The information recorded in the register and documents evidencing the conflict of interest are kept for at least 7 years.

7. PENALTIES, BREACHES AND SANCTIONS

FIAMLA

- As per s.8 of the FIAMLA, any person who commits a money laundering offence under Part II (Money Laundering Offences) of the FIAMLA shall, on conviction, be liable to a fine not exceeding 10 million rupees and to penal servitude for a term not exceeding 20 years.
- As per s.19 of the FIAMLA, any person who commits an offence relating to the obligation to report and keep records and to disclosure of information prejudicial to a request, shall be liable to a fine not exceeding 10 million rupees and to imprisonment for a term not exceeding 5 years.

FIAML REGULATIONS

- As per Regulation 33 of the FIAML Regulations, any person who commits an offence by contravening these regulations shall be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

FSC HANDBOOK

- Non-compliance with the Handbook will expose the Company to regulatory action i.e. a direction under s.7(1) (b), section 46 of the Financial Services Act 2007.
- Failure to comply with the direction shall amount to an offence under s.91 of the Financial Services Act 2007 and may further lead to sanctions imposed by the Enforcement Committee pursuant to s.53 of the Financial Services Act 2007.

To be noted that the sanctions available to the Enforcement Committee to look into breaches include:

- “issue a private warning;
- issue a public censure;
- disqualify a licensee from holding a licence or a licence of a specified kind for a specified period;
- in the case of an officer of a licensee, disqualify the officer from a specified office or position in a licensee for a specified period;
- impose an administrative penalty; and
- revoke a license.”

BREACH OF THE MANUAL

All directors, officers and employees of the Company are required to follow the policies, process and procedures outlined in this Manual. Non-adherence to provisions as laid down in the manual is subject to disciplinary actions at the discretion of Management and/or the Board.

Summary of Disciplinary Actions.

1. Oral Warning
2. Written Warning
3. Suspension
4. Dismissal