Equivest

AML/CFT COMPLIANCE MANUAL

VERSION 1.0

EQUIVEST (MAURITIUS) LIMITED

AN INVESTMENT DEALER (FULL-SERVICE DEALER EXCLUDING UNDERWRITING) LICENCE AND GLOBAL BUSINESS COMPANY LICENSED BY THE FSC

Equivest

DOCUMENT HISTORY			
Version	**Date of Changes**	**Comments**	**Date of Board Approval**
1.0	FEBRUARY 2025	The manual was drafted and submitted to the Board.	

TABLE OF CONTENTS

FOREWORD

This AML/CFT Compliance Manual (the 'Manual') contains the internal policies, procedures and control systems approved by the Board of Directors ('BoD' or 'Board' hereafter) for the good running of **Equivest (Mauritius) Limited** (''the Company'' or ''Equivest (Mauritius)''). Unless otherwise indicated, these policies, procedures and control systems are to be strictly adhered to. Any breach of the Manual will be sanctioned accordingly. No variations shall be brought to the established policies, procedures, and control systems unless the prior approval of the Board has been sought and obtained in this respect.

It is intended that the Manual will be regularly updated to reflect the enhancement brought to the internal policies, procedures, and control systems of the Company, as well as encompass any changes brought to the legal and regulatory framework governing the Company, as may be applicable.

COMPLIANCE COMMITMENT OF ALL

The BoD, the Management Team, including inter-alia, the Compliance Officer, MLRO and DMLRO are pleased to present the Company's AML/CFT Compliance Manual which details clear standards and supportive guidance that are essential for your on-the-job experiences. In addition, the AML/CFT Compliance Manual supports the Company's compliance commitment and promotes a positive, ethical environment for staff, investors/traders/clients ('clients' hereafter), partners and other stakeholders. Your adherence to the provisions of this AML/CFT Compliance Manual is essential for the effective implementation of the Company's compliance framework.

Originally adopted by the Board on September 2023, the Company's AML/CFT Compliance Manual has been revised and updated to include all changes brought to the Mauritian AML/CFT framework recently as well as recommendations contained in the Company's Compliance Audit Reports. Questions concerning the contents of this AML/CFT Compliance Manual should be referred to the Company's Compliance Officer.

We welcome your recommendations and feedback on compliance issues. The Compliance Officer remains available as a resource at any time to address your input.

SECTION 1: BACKGROUND

1.1 MAURITIUS

Mauritius is a recognized International Financial Centre offering an attractive, safe and stable business environment with a robust regulatory framework, highly qualified and multi-lingual workforce and good infrastructure, including the Information and Communications Technology infrastructure.

It ranks highly on international indices in terms of ease of doing business, African governance and economic freedom.

The Financial Services Commission ('FSC') which was established in 2001, is mandated under the Financial Services Act ("FSA") 2007 to regulate the non-banking financial services sector and the global business sector in which the company evolves.

1.2 GLOBAL BUSINESS LICENCE IN MAURITIUS

The Company holds a Global Business Licence issued under the FSA 2007. A holder of a Global Business Licence is a resident corporation, having its principal place of effective management in Mauritius, which proposes to conduct its business principally outside Mauritius.

1.3 INVESTMENT DEALER LICENCE IN MAURITIUS

An Investment Dealer Licence permits the holder to establish a trading platform in Mauritius and trade securities and similar on behalf of clients. Investment Dealer services, as all other non-banking financial services activities including the securities sector, are regulated by the FSC. The Company specifically holds an Investment Dealer (Full Service excluding Underwriting) Licence issued under the Securities Act 2005, which means that, as opposed to an Investment Dealer (Full Service including Underwriting) Licence, underwriting is not permissible.

1.4 LEGISLATIVE FRAMEWORK

- The legislative requirements and framework for a Company holding a Global Business Licence and an Investment Dealer Licence in Mauritius are set out in the Securities Act 2005 and the Securities (licensing) Rules 2007
- Income Tax Act 1995 as amended by Finance Acts and complemented by Regulations
- Companies Act 2001 as amended by Finance Acts and complemented by Regulations
- Financial Intelligence and Anti Money Laundering Act 2002 as complemented by the FIAML Regulations 2018
- Prevention of Terrorism Act 2002 as complemented by Regulations
- Prevention of Corruption Act 2002 (Repealed)

- Mutual Assistance in Criminal and Related Matters Act 2003 as amended by the relevant Finance Acts
- Banking Act 2004 as complemented by the relevant Codes and Regulations
- Financial Reporting Act 2004 as amended by Finance Acts
- Securities Act 2005 as complemented by Regulations, including The Securities (Collective Investment Schemes and Closed-end Funds) Regulations 2008
- The Securities (Collective Investment Schemes and Closed-end Funds) Regulations 2008
- Financial Services Act 2007 as complemented by Guidelines, Codes and Circular Letters
- Insolvency Act 2009
- Asset Recovery Act 2011 (Repealed)
- The Data Protection Act 2017 as complemented by Regulations
- The United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019
- The Anti-Money Laundering and Combating of the Financing of Terrorism and Proliferation (Miscellaneous Provisions) Act 2019
- FSC Guide to Fitness and Propriety
- Guidelines on The Implementation of Targeted Financial Sanctions under The United Nations (Financial Prohibitions, Arms Embargo And Travel Ban) Sanctions Act 2019 issued on 25 August 2020 by the National Sanctions Secretariat
- FSC Communique on the Guidelines on The Implementation of Targeted Financial Sanctions under The United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 issued on 25 August 2020
- FSC Anti-Money Laundering and Combatting the Financing of Terrorism Handbook 2020, last updated on 31 March 2021 and revisited in September 2022
- The Securities (Amendment) Act 2021
- Financial Crimes Commission Act 2023
- The Finance (Miscellaneous Provisions) Act 2024
- The Anti-Money Laundering and Combatting the Financing of Terrorism and Proliferation (Miscellaneous Provisions) Act 2024

1.5 COMPANY BACKGROUND

Equivest (Mauritius) Limited is incorporated in Mauritius on **1st November 2024** as a private company limited by shares. It was issued the following licences by the FSC:

- Investment Dealer (Full Service excluding Underwriting) Licence issued on **29 November 2024** under the Securities Act 2005
- Global Business Licence on **29 November 2024** under the FSA 2007

1.6 CUSTOMER / CLIENT

The Company shall onboard clients in line with the Target Markets as per its Business Plan, as amended from time to time. They may be individuals or bodies corporate.

1.7 SERVICES OFFERED

The Company shall perform such activities / duties as are customarily authorised and performed by the holder of an Investment Dealer (Full-Service Dealer excluding Underwriting) Licence under the Securities Act 2005, in particular, carrying out the following activities:

- Act or hold itself as an intermediary in the execution of securities transactions for clients;
- Trade or hold itself to trade in securities as principal with the intention of reselling these securities to the public;
- Distribute or hold itself out to distribute securities on behalf of an issuer or holder of securities;
- Solicit any investor (person or institutional or body corporate) to enter into securities transactions;
- Give investment advice which is ancillary to the normal course its business activities;
- Manage portfolios of clients.

Unless authorised by the FSC, the Company will not engage in any other activity outside the scope of its licences. The Company shall give prior written notice to the FSC of any change in its business plan.

The Company is aware that by virtue of the various types of services it offers as listed above, each of these activities and services may present different money laundering and terrorist and proliferation of weapons of mass destruction financing risks depending on factors like the customer type, source and use of funds, customer business sector and geography. Regardless of the role, Financial Action Task Force[1] ('FATF') recommends that the securities providers like the Company must continually tailor their own risk-based approach to assessing and managing ML/TF risk.

[1] *The FATF is an independent inter-governmental body that develops and promotes policies to protect the global financial system against Money Laundering, Terrorism Financing and the financing of the proliferation of weapons of mass destruction. The FATF Recommendations are recognized as the global standards in respect of AML/CFT.*

1.8 REGISTERED OFFICE

The registered office address of the Company is at C/O Credentia International Management Limited, The Cyberati Lounge, Ground Floor, The Catalyst, Silicon Avenue, 40 Cybercity, 72201 Ebène, Republic of Mauritius.

SECTION 2: COMPANY, BOARD, MANAGEMENT & STAFF

The Company's structure chart is provided at Appendix 1.

2.1 DUTIES AND OBLIGATIONS OF THE COMPANY

- As required under section 55 of the SA 2005, the Company shall file with the FSC, within 90 days of its balance sheet date, an Annual Report which shall contain the following:
    - A Report on the Corporate Governance Policy of the Company and any other related information required by the Commission;
    - Audited financial statements prepared and audited in the form and in accordance with the standards prescribed by the Financial Reporting Act and any other relevant laws of Mauritius; and
    - Any such requirement as may be specified under any other rules issued by the FSC.

Failure to abide with section 55 of the Securities Act 2005 is an offence which may give rise to a fine of up to MUR 500,000.

- In line with section 56 of the SA 2005, relating to securities transactions confirmations, the Company shall ensure the following:
    - Where the Company executes an order of a client to carry out a securities transaction, it shall send to the client without delay, a confirmation in such form as specified in the FSC Rules.
    - The Company shall send to each client a statement of account in such form and at such intervals as specified in the FSC Rules.
    - The Company shall NOT trade as principal in securities listed or traded on a securities exchange except in accordance with the applicable rules of that securities exchange.
    - Where, in respect of securities that are not listed on a stock exchange, the Company deals as a principal with a client, the Company shall, before entering into the transaction, disclose to the client that it is entering into the transaction as principal.

Contravention of any of the above is an offence under the SA 2005 which is liable to a fine of up to MUR 100,000.

- Where the Company gives investment advice, the following details, amongst others, should be kept:
    - Details on the securities on which advice will be provided;

- Whether the advice will be binding or non-binding; and
- The means through which the advice will be provided.

- Where the Company acts as an intermediary in the execution of securities transactions for clients, details on the role and function of the Company when orders are received from clients on the platform to finalisation of execution of orders (including a detailed flowchart with all the steps involved) shall be devised and maintained as part of its records. Detailed description of the activity including but not limited to the following should be kept:

    - Procedures with respect to onboarding and risk profiling of clients;
    - Details on the trading platform to be used;
    - Process and transaction flow;
    - Execution of trades;
    - Details on trade confirmations to clients; and
    - Details on monitoring of clients activity.

- With respect to trading platforms (if applicable), the Company must keep details of the following:

    - Details on the platform to be used;
    - To indicate as to whether the platform is regulated or linked to a regulated exchange;
    - Details as to how the platform operates;
    - Details as to who will have access on the platform and the rights given to them;
    - Details on the means though which the platform will be accessed; and
    - If the applicant will use the platform of another entity, indicate and keep:

        a. whether the platform provider is a regulated entity and if in the affirmative, keep evidence of same;
        b. A draft copy of agreement to be entered between the Company and the platform provider;
        c. The corporate profile of the platform provider.

- If the execution of trade will be done by a third party, the Company needs to elaborate on its responsibilities in the process. Details as to who will be responsible to issue contract notes to clients and to monitor the trade should be documented, including inter-alia:

    - A description of the monitoring process; and
    - A copy of agreement between the Company and the third party.

- The Company shall maintain adequate resources in terms of personnel, internal structures, technical and financial means as well as the required infrastructure for the nature, efficient operation of its business and future development of its activities.

- The Company shall ensure that the officers carrying on functions are fit and proper, suitably qualified and duly licensed or approved by the Regulator.

- The Company shall maintain such records and books are prescribed by the laws of Mauritius.

- The Company shall ensure that it has relevant and reasonable written policy in place to cater for conflict of interest.

- The Company shall establish procedures designed to prevent the use of insider information by an effective segregation of its activities, including to other members of the Group – which meets its obligations under the Securities (Licensing) Rules 2007. Please refer to the Privacy Policy & Internal Privacy Controls in this respect.

- The Company's systems and procedures in place shall ascertain that investment decisions concerning the portfolio of clients shall not be communicated or be (made) available to any unauthorised third party. Likewise, the systems and procedures shall ensure that non-public information is strictly controlled and not circulated to any unauthorised parties. Please refer to the Privacy Policy & Internal Privacy Controls in this regard.

- The Company shall NOT undertake any investment transaction, if, to its knowledge, having made all reasonable enquiries, it would result in a breach of any restriction as provided under any relevant law.

- The Company has established detailed AML/CFT procedures and processes through this AML/CFT Compliance Manual – which satisfies its obligation under the Securities (Licensing) Rules 2007.

2.2 DUTIES AND RESPONSIBILITIES OF THE BOARD OF DIRECTORS

The Company is managed by a Board of Directors ('the Board' or 'BoD') who has overall responsibility for its operations. The Board shall consist of at least two directors who are resident in Mauritius. The Company shall at all times ensure that it meets the requirements of section 133 of the Companies Act 2001 and section 24 of the FSA 2007 in terms of the constitution and qualification of its Board. The Board shall adhere to their duties and responsibilities as set out under section 143 of the Companies Act 2001 at all times.

With regard to AML/CFT matters, the Board shall be responsible to:

(a) Maintain accountability and oversight for establishing AML/CFT Framework and minimum standards;

(b) Approve policies regarding AML/CFT measures within the Company, including those required for risk assessment, mitigation and profiling, CDD, record keeping, on-going due diligence, reporting of suspicious transactions and combating the financing of terrorism/proliferation;

(c) Establish appropriate mechanisms to ensure the AML/CFT Framework is periodically reviewed and assessed in line with changes and developments in the Company's services, technology as well as trends in ML/TF;

(d) Establish an effective internal control system for AML/CFT and maintain adequate oversight of the overall AML/CFT measures undertaken by the Company;

(e) Define the lines of authority and responsibility for implementing the AML/CFT measures and ensure that there is a separation of duty between those implementing the policies and procedures and those enforcing the controls;

(f) Ensure an independent audit function to assess and evaluate the robustness and adequacy of controls implemented to prevent ML/TF;

(g) Establish Management Information System that is reflective of the nature of the Company's operations, size of business, complexity of business operations and structure, risk profiles of products and services offered and geographical coverage; and

(h) Appoint a MLRO, a Deputy MLRO ('DMLRO') - who shall exercise the MLRO's functions in the latter's absence and shall have similar status, duties, responsibilities, and experience to the MLRO in respect of AML/CFT - and a Compliance Officer ('CO').

(i) Assess the implementation of the approved AML/CFT Framework through regular reporting and updates by the Management / (D)MLRO / external compliance auditor;

Additionally, the Board shall be responsible to:

(a) Recruit staff of appropriate calibre who will be capable of discharging their responsibilities diligently.

(b) Ensure the integrity of all employees by establishing appropriate employee assessment system.

2.3 DUTIES AND RESPONSIBILITIES OF THE MANAGEMENT COMPANY

In accordance with section 71(3)(a)(iii) of the Financial Services Act 2007 ('FSA'), the Company is administered by a Management Company, namely **Credentia International Management Limited (''CREDENTIA'' or ''the Management Company''** hereafter), also licensed and regulated by the FSC. While the Board remains responsible for all of the Company's compliance functions, the Company has delegated some of its roles and duties to CREDENTIA. This delegation of some of its functions is covered under the Service Level Agreement established between the Company and its Management Company. For more information in this regard, please refer to Service Level Agreement.

The Company is supported by its Management Company which conducts the day-to-day administrative functions of the Company. Consequently, compliance with legal requirements relating to the operations of the Company is carried out by the Management Company, in line with contractual

agreements or by regulation, which also implements appropriate anti-money laundering procedures for the Company.

The Board shall ensure that any of the Officers designated and appointed and/or its staff (if applicable) is 'fit and proper' and in this context, the Company relies on its Management Company to cause the conduct of a screening of any new candidate selected for designation prior to his/her appointment as well as carry on-going due diligence checks on existing Officers and staff, as described at section 2.9 below.

2.4 DUTIES AND RESPONSIBILITIES OF THE INVESTMENT DEALER TEAM

The strength of the investment dealer team is a key component of the smooth and efficient running of the Company given its Investment Dealer Licence. The Company shall therefore ensure that it holds adequate information on its members and be in a position to demonstrate their suitability to discharge their responsibilities.

The Company must ensure that at least 2 members are appointed on the Investment Dealer Team to ensure business continuity. These persons may be regulated or hold a licence from a regulated authority.

In any case, members of the investment dealer team must have relevant experience and qualification as required under the Securities Act 2005 and must demonstrate a proven track record in the provision of investment dealer services.

The duties and responsibilities of the Investment Dealer Team shall be as per Appendix 4.

2.5 DUTIES AND RESPONSIBILITIES OF THE MONEY LAUNDERING REPORTING OFFICER ("MLRO") AND THE DEPUTY MLRO

The MLRO / DMLRO shall be the officers 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.

The Company has designated Senior Officers of its Management Company who have been duly approved by the FSC as its MLRO and DMLRO respectively.

The MLRO / DMLRO shall have the technical skills required to make an assessment of internal reports prior to determining whether a report should be filed with the FIU.

The duties and responsibilities of the MLRO and DMLRO shall be as per Appendix 2.

At each Board Meeting, but at least once per year, the MLRO / DMLRO shall report to the Board of the Company on any material breaches of the internal AML/CFT policy and procedures and of the AML/CFT laws, codes, and standards of good practice, as applicable.

2.6 DUTIES AND RESPONSIBILITIES OF THE COMPLIANCE OFFICER

The Compliance Officer ('CO') is generally responsible for the implementation and ongoing compliance of the Company with internal programmes, controls and procedures and requirements of the laws and regulations.

The Company has designated a Senior Officer of its Management Company who has been duly approved by the FSC as its CO.

The duties and responsibilities of the Compliance Officer shall be as per Appendix 3.

At each Board Meeting, but at least once per year, the CO shall also report to the Board of the Company on any material breaches of the internal AML/CFT policy and procedures and of the AML/CFT laws, codes and standards of good practice, as applicable.

2.7 DUTIES AND RESPONSIBILITIES OF ALL STAFF AND DESIGNATED OFFICERS

- All officers of the Company, employees as well as the staff of the Management Company assigned to administer the Company shall adhere to this AML/CFT Compliance Manual and regulatory requirements applicable to the Company. Failure of adherence shall constitute misconduct on the part of the officers / staff and shall be reported to the Management Company and dealt with by the latter in accordance with Disciplinary Measures as provided under 2.11 below.

- They shall also abide to the constitutive documents of the Company, apply rules, regulations, and laws, including but not limited to the Securities Act 2005, The Securities (Collective Investment Schemes and Closed-end Funds) Regulations 2008 and AML / CFT policies, procedures, rules, regulations, and laws governing the Company. Failure of adherence shall constitute misconduct on the part of the staff, officers and directors of the Company and shall be dealt with by the Company in accordance with the Disciplinary Measures under Section 2.11.

- They shall be fully informed of the Company's position on money laundering and terrorist financing and their responsibilities to report suspicious cases, including whistle blowing in instances involving suspicion of illegal or dishonest activities observed within the Company. The whistle blower is not responsible for investigating the activity or for determining fault or corrective measures. The Director(s)/Compliance Officer/MLRO/DMLRO will do the needful once informed of the situation.

- They shall practise staff vigilance to drive early detection and avoidance of money laundering and terrorist financing.

- They must Immediately report suspicious activities/transactions to the MLRO / DMLRO.

- They must ascertain that the Compliance Officer / MLRO / DMLRO has full access to all relevant information that may be of assistance.

2.8 APPOINTMENT AND CHANGES OF OFFICERS

An Officer is a member of the Board, a Chief Executive, a Managing Director, a Chief Financial Officer or Chief Financial Controller, a Manager, a MLRO/DMLRO, a Compliance Officer, a Company Secretary or a Member of the Investment Dealer Team.

The Company shall adhere to the FSC Guide to Fitness and Propriety and the provisions of section 24 the FSA 2007 in this respect. Accordingly, all Officers of the Company must be fit and proper and appointments / changes of key personnel must be approved by / notified to the FSC.

The Company shall, through the Management Company, seek the approval of the FSC prior to the appointment of any Officer. An application for approval shall be submitted to the FSC along with the full particulars, including a duly signed Personal Questionnaire (PQ) Form of the person to be appointed.

Similarly, the Company shall inform the FSC of any resignation or removal of an Officer and the circumstances surrounding such request for resignation or removal.

2.9 EMPLOYEE SCREENING PROCEDURES

In accordance with regulation 22(1)(b) of FIAML Regulations 2018, the Company shall ensure high standards when hiring employees. In this respect, the Company has adopted the following procedures:

- Obtaining and confirming employment history, qualifications and professional memberships of the employee.
- Obtaining and confirming appropriate references;
- Obtaining and confirming details of any regulatory action or action by a professional body taken against the prospective employee;
- Obtaining a certificate of character on an employee;
- Screening the employee at selection stage, encompassing checks against the UN and National Sanctions List of designated or listed parties as per the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019.

Screening of employees shall be triggered by the Management Company. The Management Company is expected to ascertain that the search engine used for the conduct of the screening includes searches against United Nations Security Council and domestic List of Targeted Financial Sanctions.

2.10 AML/CFT TRAINING & OTHER RELEVANT TRAINING

The Company shall have in place 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:

- assist them in recognizing transactions and actions that may be linked to money laundering or terrorism financing;
- instruct them in the procedures to be followed where any links to money laundering or terrorism financing have been identified.

The Company shall ensure that the designated CO/MLRO/DMLRO fulfil the requirement of Continuous Professional Development ('CPD') annually, as applicable to them under the Competency Standards issued by the FSC in October 2014.

Additionally, besides, the AML/CFT refresher courses, the training programme shall include the provision of training dedicated to the Investment Dealer Team relevant to their roles.

A Training log (See Appendix 8) shall be maintained in this regard by the Compliance Officer and must encompass all internal and external training followed by all the principals and officers of the MC servicing the Company.

2.11 DISCIPLINARY MEASURES

Any breach of this Manual shall be considered as serious. Any breach or misconduct by a director, an Officer, employee of the Company or staff of the Management Company assigned to administer the Company shall be referred to the Board which shall decide upon the disciplinary measure to apply in any given scenario. Disciplinary measures and sanctions applied shall be commensurate with the gravity of the breach or misconduct, including inter-alia, the termination of the employment Agreement and/or legal action(s) as provided under the Workers' Rights Act, as may be applicable.

SECTION 3: GENERAL POLICIES AND PROCEDURES

3.1 RECORDS KEEPING

3.1.1 PURPOSE AND SCOPE

The purpose of this policy regarding recordkeeping (this "Policy") is to ensure that the Company implements and maintains appropriate procedures for cataloguing and preserving its books and records in accordance with applicable laws (3.1.2 below refers).

The objective of record keeping is to ensure that the Company can provide necessary information about Customers, and their transactions details at any given time or as per the request for FSC, FIU, Law Enforcement Agencies, Courts, Auditors/Examiners, or any competent authorities. Pursuant to Section 17(b) of FIAMLA 2002 requires the Company to maintain records. Failure to comply is regarded very seriously by the FIU and may result in regulatory and/or criminal sanctions.

This Policy outlines the types of books and records that shall be maintained by the Company, how the Company shall catalogue and maintain such books and records, and who is responsible for maintaining them. All records will be kept for a minimum period of at least seven (7) years from the date of the relevant event or, in the case of an ongoing business relationship, after the business relationship ceases, in a form which is immediately accessible upon request.

3.1.2 LEGAL REQUIREMENT FOR RECORDS KEEPING

The Company shall maintain company records in accordance with the following:

- Section 190(2) of the Companies Act 2001
- Section 29 of Part V (ongoing obligations of licensees) of the Financial Services Act 2007
- Section 71 (4)(b)(iii) of the Financial Services Act 2007
- Section 17F of the Financial Intelligence and Anti-Money Laundering Act
- Regulation 14 of the FIAML Regulations 2018
- Chapter 11 of the FSC Handbook; and
- Any other Acts and / or Regulations, as applicable

The Company is committed to complying in all respects with applicable laws and regulations regarding recordkeeping.

3.1.3 GENERAL RECORDS KEEPING POLICY

Recommendation 11 of the Financial Action Task Force (FATF) requires financial institutions to have proper and effective policies, procedures, and controls in place to ensure that record of transactions is maintained during, as well as, after the course of the business relationship. In Mauritius, it is provided by Chapter 11 of the FSC Handbook, as well as Section 190 of the Companies Act, that all records obtained through CDD measures, records of transactions (domestic or international) and copies of suspicious transactions reports shall be maintained for a period of at least 7 years. Record keeping, is an essential component of the AML and CFT regime because it acts as evidence that the company is compliant with regulatory obligations and provides assistance to law enforcement agencies in conducting financial investigations upon request.

The Management Company shall keep all records of the Company in Mauritius at its registered office address and accordingly the Internal Procedures Manual which elaborate on Records Keeping Policy shall be applicable.

The Company shall maintain true, accurate, and current records that are well organized at all times. The Company is at all times subject to surprise examinations of its books and records by the FSC and other governmental authorities.

It is a violation of law to forge, falsify, tamper with, obliterate, or prematurely destroy these records. Doing so could subject the personnel involved to criminal penalties, regulatory sanctions and/or termination of employment.

3.1.4 RESPONSIBILITY FOR RECORDS KEEPING

The Management Company, looking into the day-to-day administrative affairs of the Company, has the overall responsibility for the implementation and monitoring of our books and records policy and recordkeeping requirements for the Company. The Management Company will upon request by a regulatory authority, provide copies of these records in the medium and format in which they are stored, as well as printouts of such records; and a means to access, view, and print the records if required.

3.1.5 FORMAT AND RETRIEVAL OF RECORDS

The Company shall maintain a filing system that provides for organisation of its books and records sufficient to allow their retrieval within a reasonable amount of time.

In view of the size and business's record storage procedures, the Company shall keep its records in any format listed below:

- Original hard copy documents
- Scanned form - scan the verification material and hold it electronically

- Certified true copies kept either in hard or soft of original hard documents
- Keep electronic copies or hard copies of the results of any electronic verification checks
- Record reference details of the any material kept.

Regardless of the form in which the Company chooses to keep records, correspondence records must be sufficiently detailed to enable a transaction to be readily reconstructed at any time. For certification details, please see Section 5.12.

3.1.6 RECORD RETENTION

All documents will be recorded for a minimum period of seven (7) years from the date of the termination of the client / business relationship.

The procedures in this regard are included in the Internal Procedures Manual, adopted by the Company.

Where the records are being held electronically, the Company should ensure that the working documents should be legible and in a usable filing system, so that they can be retrieved/found without undue delay and produced on a timely basis especially where the originals are not to be retained.

Where the records are received in a language other than the official languages (English & French), the Company must ascertain that the documents are duly translated in either English or French and that the translator is right and proper to fulfil such a function. Evidence of the foregoing must be kept on record.

3.1.7 OTHER LOGS AND REGISTERS

The Company must make and keep true, accurate, and current records relating to its investment dealings business. Furthermore, the Company must have in place records as specifies under Chapter 11 of the FSC Handbook and Section 17F of FIAMLA. The MC on the other hand, must maintain those records in accordance with the required retention/cover periods, which generally fall into the category of 'Log and Register'. This following register are held at the Registered Office of the Company:

- Training Register
- PEP Register containing details of PEPs (if any).
- STR Log (Internal & External)
- List of False Positive and Positive Matches
- List of Rejected Clients
- Complaints Register
- Breach Reporting Register
- Register of Interests
- List of Service Providers / Third Parties
- Special Case Logs or Exceptions Report

- Transaction Monitoring Sheet
- Log of Reporting on Positive Name Matches under section 25(2) of the UN Sanctions Act 2019
- Log of Notifications to the NSSEC, the FIU, the FSC under section 23(4) of the UN Sanctions Act 2019

3.2 ANNUAL REPORT AND CORPORATE GOVERNANCE REPORT

3.2.1 STATUTORY FILINGS AND COMPLIANCE REPORTS

The Company's Management Company shall make payments of annual fees to the respective authorities such the Registrar of Companies ('ROC') and the Financial Services Commission ('FSC') and keep a copy of the receipts for compliance purposes.

The Company is responsible for preparing its financial statements in accordance with:

- Section 210 of the Companies Act 2001,
- Section 30 of the FSA 2007,
- The Securities (Amendment) Act 2021 and
- Accounting standards issued and / or regulations made under the Financial Reporting Act 2004.

As per Circular Letter CL280218 issued by the FSC on 28 February 2018, the Company is required to present a Corporate Governance Report. The Report together with the audited financial statements ('AFS') of the Company is required to be submitted to the FSC not later than 90 days after the expiry of each balance sheet date.

The Accounts/Financial Auditor of the Company will be approved at each Annual Meeting of the Company in accordance with section 195 of the Companies Act 2001 ('CA2001').

The Company's Management Company bears the statutory duty of the filings of documents and settlement of statutory fees and charges on its behalf as follows:

- Filing of its audited financial statements within 90 days after the close of financial year in accordance with Section 55 of the Securities Act 2005
- Payment of the annual FSC licence fee and Registrar of Companies ('ROC') annual fee in respect of the Company's GBC Licence in accordance with the FSA 2007 and the CA2001
- Filing of appointment / changes in directors for the Company in accordance with CA2001 and the FSA 2007
- Filing of changes in the capital structure of the Company (if applicable) in accordance with CA 2001 and FSA 2007
- Filing of tax returns of the Company in accordance with section 116 of the Income Tax Act 1995
- Filing of charges of the Company, as may be needed, in accordance with CA2001

- Reporting under the US Foreign Account Tax Compliance Act and/or the OECD Common Reporting Standard ('FATCA/CRS'), as may be required, in accordance with the Mauritius Income Tax Act
- Registration and Obligations under the Data Protection Act 2017, which came into effect on 15 January 2018

While the Company's Management Company is responsible to ensure that the Company adheres to the above requirements at all times, the Compliance Officer shall also report on any such failure at the Company's Board within its Compliance Report. Any continual non-compliance with any of the above requirements shall be reviewed and appropriate decisions shall be made accordingly by the Board. The Compliance Officer will then implement any decisions taken by the Board, as may be required. The reports and decisions / actions taken shall then be presented at the subsequent Board Meeting.

3.2.2 GOOD GOVERNANCE MEASURES

The Company is committed to observing high standards of Corporate Governance, and report on its compliance with the principles set out in the National Code of Corporate Governance as required under Circular Letter CL280218 issued by the FSC on 28 February 2018. Furthermore, Condition 5 of the GBC Licence states that the Company shall devise and set-up appropriate corporate governance measures for the sustainability of the Company and shall review and re-assess these measures from time to time.

In this regard, the Company's Corporate Governance Policy will be used. The measures contained therein shall take precedence and shall be evaluated and re-assessed from time to time.

3.3 CLIENT PAYMENT INSTRUCTIONS

The Company shall continuously review, supervise, rebalance, and administer the investment programme of any of its client, as may be required.

Any instructions for inward and/or outward transfer of funds into/from the clients' accounts held through banks/financial institutions for investment purposes, within the scope of the Client Agreement established between the Company and any one client, will be effected by the Administrator, in collaboration with the Investment Dealer Team.

NO-CASH POLICY

The Company has implemented a strict zero tolerance policy against cash deposits including ATM Cash deposits / Cheque Deposits in order to adhere to Anti-Money Laundering (AML) standards and for its commitment to regulatory compliance.

3.4 CLIENT INSTRUCTION

The Company acts within the scope of the Client Agreement established between the Company and its clients. The Company maintains transactional access to the clients' banks and financial institutions to carry out its licensed activities.

- The clients shall indemnify the Company and their directors, officers, and employees against any and all losses paid, suffered or incurred by the Company or their directors, officers or employees, directly or indirectly arising as a result of;

  (i) the performance by the Company under the service agreement in place, or
  (ii) carrying out or relying on any Instructions and any information provided or made available to the Company by the clients, their Custodian, their Administrator, or any of their agents, except to the extent that such Losses result directly from the negligence, wilful default or fraud of the Company or of its directors, officers or employees in providing the services under this agreement.

- Regardless of the method used to translate a verbal instruction into a written confirmation, the ultimate objectives are two-fold: to be able to keep reliable record/evidence of same to enable a transaction reconstruction at any point in time as required under the FIAMLR 2018 and the FSC Handbook and to sustain indemnity cover.

3.5 TRANSACTION MONITORING THROUGH RECONCILIATION OF THE CLIENT & CORPORATE BANK ACCOUNTS

The Company has opened bank accounts in Mauritius. View access has been granted to the resident directors for bank accounts held in Mauritius. Real time monitoring is conducted by the Operations Team and then shared with the Management Company. Please refer to Appendix 17 – Transaction Monitoring.

The normal frequency for this reconciliation exercise is fortnightly basis but the frequency may be increased upon the request of the clients it manages or as may be required.

The process for reconciliation is as follows:

3.5.1 LOCAL BANK

Any payment instructions (deposits and/or withdrawals) received, the Banks liaise with the Management Company to request for supporting documents.

Upon satisfactory verification and due diligence, the transaction is processed.

3.5.2 FOREIGN BANK

The transaction monitoring will be carried out on a fortnightly basis depending on the volume of transactions.

Any deposit or withdrawal made by investors/traders/clients either through local / foreign banks or Payment Service Provider as applicable – the real time monitoring is carried out by the Operations Team/Dealing Team of the Investment dealer.

Thereafter, depending on the volume of transactions, the Administrator/Compliance Analyst/Management Company requests the transaction reports on either daily, weekly, or monthly basis for a second verification.

The Compliance Officer shall verify the transactions being monitored and reconciled on a risk basis as part of the ongoing Client file reviews and customer due diligence. The MLRO shall also check the quarterly transactions and reconciliation reports during his/her quarterly visits and report on same in his/her Reports to the Company's Board annually.

3.6 SYSTEMS BACK-UP, BUSINESS CONTINUITY AND DISASTER RECOVERY PLANS

It is the Company's policy to have all files backed in soft copy and it is essential that a system back-up is done regularly so that no information is lost in case of any technical failure. The back-up is covered under the Company's Internal Procedures Manual which elaborate on Records Keeping Policy and its Information Technology & Security Manual which it has adopted.

The Company has adopted a Business Continuity and Disaster Recovery Plan (BCDRP). Please also refer to the Business Continuity and Disaster Recovery Plan for more information.

The main objectives of the BCDRP is to ensure that in case of material business disruptions the Company resumes its operations with minimal interruptions and in the most efficient manner possible. That said, the BCDRP has been adapted to the Company's business set up.

For an Investment Dealer licensee, bearing in mind the extent to which the whole business set up rests on its trading platform, online on-boarding and trade execution, the Company is recommended to have in place:

1. Contingency plan – stretching on response and recovery strategies of where the Companies' key documents, records and equipment may be retrieved in an emergency to aid in the disaster recovery process.

2. IT Policy, IT Penetration Test and IT audits – the Company should also arrange to conduct IT audits regularly (every year) and address identified loopholes. IT penetration test should be

performed to ensure that its systems are not vulnerable or susceptible to cyber-attacks. Details of the frequency of back-ups should also be included.

Based on the foregoing, an Information Technology & Security Manual has been established in this regard to complete and sustain the BCDRP. The BCDRP is reviewed and documented annually.

An IT audit generally follows the same pattern as a typical financial statement audit. There are four primary phases of the audit which are planning, tests of controls, substantive tests, and audit completion/reporting. During the financial year end audit, the auditors normally carry out an IT audit. The Company can also opt to have a full-fledged IT Audit under a separate cover whereby they will have a full report at the end of the process.

The IT audit normally covers the following:

1. Data back up and archiving procedures
2. Business Continuity Planning
3. Disaster recovery plan
4. User Acceptance policy
5. Password Policy
6. E-mail Policy
7. Internet Usage Policy
8. Social medial usage Policy
9. Asset Management Policy
10. MetaQuotes

On the other hand, clients also use MetaQuotes, which is a reputed supplier of the most reliable modern software solutions for financial markets. Their core focus is the development and implementation of professional, high quality online trading platforms for automated online brokerage services and online management systems.

MetaQuotes sticks to high security requirements to ensure the secure exchange of confidential data through the app, including images, videos, and different document types. This software is safe to use since all transmitted information is securely encrypted.

In case, clients will not opt for IT audits, they can provide a profile/certificate to authenticate the secureness of the software.

3.7 CODE OF ETHICS

The Company shall follow the Code of Conduct and Ethics of the Company. In addition to any other duties and obligations imposed upon by the Company, the latter expects all Board Members, officers servicing it and staff to abide to the following principles:

a. act with integrity, competence, diligence, respect and in an ethical manner with the public, clients, prospective clients, employers, co-employees, and other participants in the business;

b. ensure the Company's interests are protected and trading clients' requests in terms of their transactions, deposits, monitoring are in line with prevailing laws and regulations;

c. preserve the confidentiality of all information communicated by clients within the scope of the Company-client relationship, except where the Company is required, by law, to report to relevant authorities, any suspected illegal activities by clients;

d. refuse to participate in any business relationship or accept any gift that could reasonably be expected to affect their independence, objectivity, or loyalty to clients;

e. use due diligence and care and exercise independent professional judgment when engaging in their professional activities;

f. practice and encourage others to practice in a professional and ethical manner that will reflect credit on the employees and the profession;

g. promote the integrity of, and uphold the rules governing capital markets;

h. maintain and improve its professional competence and strive to maintain and improve the competence of other investment professionals;

i. act in a professional and business-like manner at all times; and

j. ensure that the policies, procedures, and processes adopted by the Company are always adhered to, failing which sanctions will be taken.

In the event of a breach, the company shall first of all investigate the severity of the breach, and may apply hereunder measures/sanctions:

- Disciplinary Committee and/or HR Committee
- Re-assignment of duties
- Issue warning letters
- Remove certain access
- Suspension
- Termination of employment

Note: It is also mandatory to record the sanction decision and advice of the outcome.

3.8 INSURANCE POLICY

In accordance with the prudential and safeguarding requirements as laid down by the FSC under its licensing criteria applicable to Investment Dealer Licences, the Company is required to subscribed to a Professional Indemnity Cover ('Insurance Cover') and Directors & Officers Liability **(Optional)** and be sheltered against the following risks amongst others:

- Fraudulent activities of employees.
- Fraudulent instructions.
- Losses arising from the malicious or fraudulent corruption of electronic data or electronic transactions.

- Legal liability to third parties arising from breaches of professional duty.

The Company need to make sure that it holds a valid insurance cover, or it renews the cover in a timely manner so that the licensing criteria is met at all times.

3.9 MINIMUM CAPITAL

By virtue of its Investment Dealer (Full Service excluding Underwriting) Licence, the minimum stated unimpaired capital of the Company as defined under the Fourth Schedule (Rule 14) of the Securities (Licensing) Rule 2007 is MUR1 million only. The unimpaired stated capital shall be fully paid, and no amount shall be due or payable at any point of time.

Should the minimum stated unimpaired capital of the Company fall below the required amount, the Company shall inform the FSC forthwith and do the needful as required.

3.10 ADVERTISEMENT

The Company will not issue or participate in or knowingly allow its name or its business to be used in respect of any advertisement, sales literature or correspondence which:

- Contains any untrue statement or omission of a material fact or is otherwise false or misleading.
- Contains unjustified promise of specific results.
- Uses unrepresentative statistics to suggest unwarranted or exaggerated conclusions or fails to identify the material assumption made in arriving at these conclusions.
- Contains any opinion or forecast of future events which is not clearly identified as such.
- Fails to fairly present the potential risks to the investors.
- Is detrimental to the interests of the public.
- A copy of any advertisement or sales literature proposed to be issued by the Company shall be submitted to the FSC before it is issued.

The Company shall in any case abide with the FSC Guidelines for Advertising and Marketing of Financial Products in this respect and seek the FSC's approval wherever required.

3.11 DATA PROTECTION

The Company shall be governed by the provisions of the Data Protection Act 2017, including the Regulations made thereunder.

In this context, the Company shall registered as Data Controller with the Data Protection Office as required under the Data Protection (Fees) Regulations 2020 – the Communique to the Public issued by The Data Protection Commissioner on 20th July 2020 refers.

It shall be appointed a designated Data Protection Officer ('DPO') who is a staff of its Management Company and adopt the Data Protection Framework of CREDENTIA.

The Privacy Policy & Internal Privacy Controls – see 3.11.1 below - shall include a comprehensive Data Protection Framework in accordance with the Mauritius Data Protection Act 2017.

3.11.1 OFFICE SECURITY, CONFIDENTIALITY AND CONSULTATION OF DOCUMENTS

Access to the Company by visitors is strictly controlled at the main entrance by CREDENTIA which will apply its own office security rules to the Company.

Unless required by law, the Company will not disclose any documents or information on its matters or clients' matters. All officers of the Company and staff of CREDENTIA servicing it should ensure that all business matters relating to the Company and its clients are treated professionally and with discretion.

Moreover, the Company has a well-documented Privacy Policy & Internal Privacy Controls in place, which all employees must follow. The framework includes a detailed description of the measures that must be implemented to ensure the confidentiality, security, and safety of client information and records.

3.12 SUBSTANCE REQUIREMENT – LICENSING CRITERIA

The Company is committed to fulfil its substance requirements in accordance with section 71(3)(a) of the FSA 2007 which requires a holder of a Global Business Licence to at all times carry out its core income generating activities in, or from, Mauritius, the licensing criteria governing its business and the Circular Letter (CL1-121018) issued by the Commission on 12 October 2018 as soon as it starts its operations.

Additionally, provision will be made in its Constitution to the effect that arbitration will be done in Mauritius in case of commercial disputes – which shall further substantiate this licensing criteria.

SECTION 4: ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM AND PROLIFERATION POLICY & PROCEDURES ('AML/CFT')

Through this Manual, the Company has put in place policies, procedures, and processes with respect to combating money laundering and terrorist/proliferation financing ('ML/TF') that are deemed appropriate based on the nature of the business of the Company.

In devising the AML/CFT related policy and procedures, the Company has given due consideration to the applicable legal framework which includes, but is not limited to the following:

- The Financial Intelligence and Anti-Money Laundering Act 2002, and any regulations made thereunder, including the Financial Intelligence and Anti-Money Laundering Regulations 2018 and amendments thereof
- The United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 (The "UN Sanctions Act 2019")
- The Prevention of Terrorism Act 2002
- The Convention for Suppression of the Financing Terrorism Act 2003
- The Securities Act 2005 and any regulations made thereunder, including The Securities (Collective Investment Schemes and Closed-end Funds) Regulations 2008 and amendments thereof
- The Anti Money Laundering and Combatting the Financing of Terrorism and Proliferation (Miscellaneous Provisions) Act 2019
- The Anti Money Laundering and Combatting the Financing of Terrorism and Proliferation (Miscellaneous Provisions) Act 2020

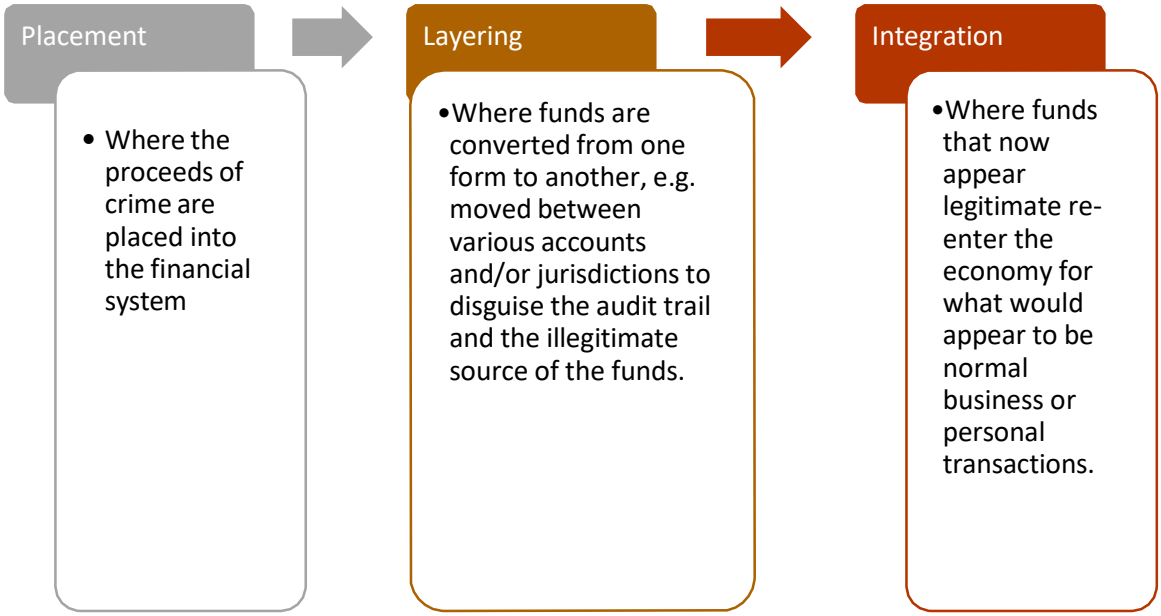
In addition, the Company shall also follow guidance issued by international bodies like the FATF that are relevant and useful to combat money laundering and financing of terrorism / proliferation.

4.1 MONEY LAUNDERING

In general terms, Money Laundering is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of criminal activities.

If successful, the criminal property can lose its criminal identity and appear legitimate, meaning that criminals can benefit from their crimes without the fear of being caught by tracing their money or assets back to a crime.

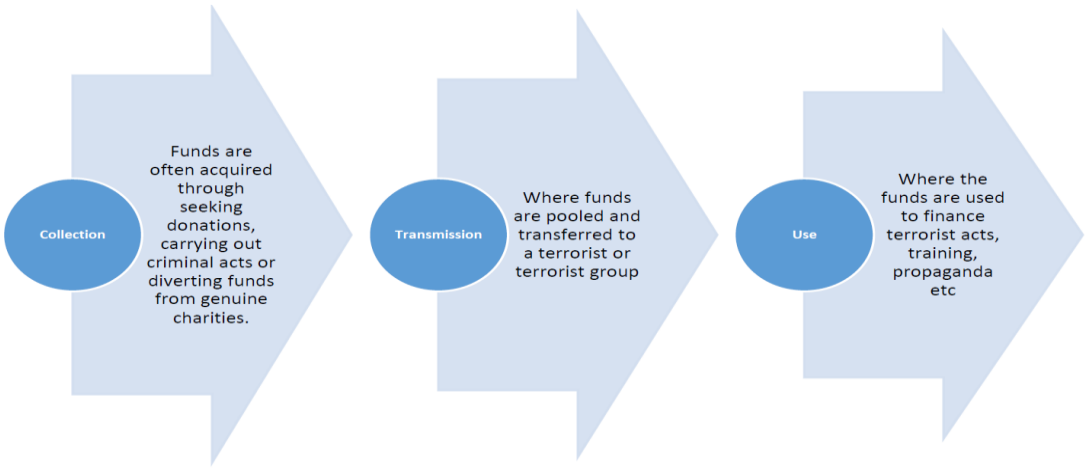
Money Laundering will often involve a complex series of transactions, traditionally represented in three separate phases.



4.2 TERRORISM FINANCING

In a nutshell, Terrorism Financing is the financial support, in any form, of terrorism or those who encourage, plan or engage in terrorism. Terrorism Financing differs from Money Laundering in that the source of funds can either be legitimate, such as an individual's salary, or illegitimate, like the proceeds of crimes such as selling pirate DVDs, fraud or drug trafficking.

Terrorism financing often involves a complex series of transactions, generally considered as representing three separate phases and this could be sourced through various means for example through seeking donations, carrying out criminal acts and from genuine charities, as illustrated below:



4.3 PROLIFERATION OF WEAPONS OF MASS DESTRUCTION FINANCING

Proliferation of weapons of mass destruction ('WMD') 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 organizations or acting as representatives or middlemen.

4.4 SUMMARY OF OFFENCES RELATING TO MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION FINANCING:

It should be noted at the outset that US anti-money laundering laws, in particular the US Patriot Act 2001 (as amended), have an extra-territorial effect and where a business deals in the US Dollar, there is a risk that US regulations and sanctions may also apply.

The pieces of legislation listed below make up the local AML/CFT framework and offences related to money laundering and terrorist financing are contained in FIAMLA and FIAML Regulations. The following is a non-exhaustive list of offences for ease of reference.

- **Section 3 of FIAMLA states:**

(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.

(2) A bank, financial institution, cash dealer or member of a relevant profession or occupation that fails to take such measures as are reasonably necessary to ensure that neither it nor any service offered by it, 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.

(3) In FIAMLA, reference to concealing or disguising property which is, or in whole or in part, directly or indirectly, represents, the proceeds of any crime, shall include concealing or disguising its true nature, source, location, disposition, movement, or ownership of or rights with respect to it.

- **Section 4 of FIAMLA states:**

Without prejudice to section 109 of the Criminal Code (Supplementary) Act, any person who agrees with one or more other persons to commit an offence specified in section 3(1) and (2) shall commit an offence.

- **Section 5 of FIAMLA states:**

(1) Notwithstanding section 37 of the Bank of Mauritius Act 2004, but subject to subsection (2), any person who makes or accepts any payment in cash in excess of 500,000 rupees or an equivalent amount in foreign currency, or such amount as may be prescribed, shall commit an offence. (2) Subsection (1) shall not apply to an exempt transaction.

- **Section 8 of FIAMLA states:**

(1) Any person who –

(a) commits an offence under this Part; or
(b) disposes or otherwise deals with property subject to a forfeiture order under subsection (2), shall, on conviction, be liable to a fine not exceeding 2 million rupees and to penal servitude for a term not exceeding 10 years.

(2) Any property belonging to or in the possession or under the control of any person who is convicted of an offence under this Part shall be deemed, unless the contrary is proved, to be derived from a crime and the Court may, in addition to any penalty imposed, order that the property be forfeited.

(3) Sections 150, 151 and Part X of the Criminal Procedure Act and the Probation of Offenders Act shall not apply to a conviction under this Part.

- **Section 16(3) (A) of FIAMLA states:**

Legal consequences of reporting

Any person who fails to comply with subsection (1) shall commit an offence and shall, on conviction, be liable to a fine not exceeding 5 million rupees and to imprisonment for a term not exceeding 10 years.

- **Section 17(C) (6) of FIAMLA states:**

Customer due diligence requirements

Any person who knowingly provides any false or misleading information to a reporting person in connection with CDD requirements under the FIAMLA or any guidelines issued under this Act shall

commit an offence and shall, on conviction, be liable to a fine not exceeding 500, 000 rupees and to imprisonment for a term not exceeding 5 years.

- **Section 19 of FIAMLA states:**

Offences relating to obligation to report and keep records and to disclosure of Information prejudicial to a request;

(1) Any bank, cash dealer, financial institution or member of a relevant profession or occupation or any director, employee, agent or other legal representative thereof, who, knowingly or without reasonable excuse –

(a) fails to –

(i) supply any information requested by the FIU under section 13(2) or 13(3) within the date specified in the request;
(ii) make a report under section 14; or
(iii) Any person who fails to comply with sections 17 to 17G shall commit an offence and shall, on conviction, be liable to a fine not exceeding 10 million rupees and to imprisonment for a term not exceeding 5 years.

(b) destroys or removes any record, register or document which is required under FIAMLA or any regulations;

(c) facilitates or permits the performance under a false identity of any transaction falling within this Part, shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

(2) Any person who –

(a) falsifies, conceals, destroys or otherwise disposes of or causes or permits the falsification, concealment, destruction or disposal of any information, document or material which is or is likely to be relevant to a request to under the Mutual Assistance in Criminal and Related Matters Act 2003; or

(c) knowing or suspecting that an investigation into a money laundering offence has been or is about to be conducted, divulges that fact or other information to another person whereby the making or execution of a request to under the Mutual Assistance in Criminal and Related Matters Act 2003 is likely to be prejudiced, shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

- **Section 19E of FIAMLA states:**

Duty to provide information

Any person who fails to comply with a request made under subsection (2)(b) shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

- **Regulation 33 of FIAML Regulations states:**

Any person who contravenes these regulations shall commit an offence and shall on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

4.5 AML/CFT POLICY AND PROCEDURES

4.5.1 RISK ASSESSMENT POLICY

The FATF Recommendations provide for AML/CFT requirements, allowing a business to adopt a risk-based approach towards the prevention and detection of ML/TF. The application of a risk-based approach provides a strategy for managing potential risks through commensurate preventive and mitigating measures, enabling the Company to subject clients to proportionate controls and oversight in the most cost-effective way.

In accordance with section 17 of FIAMLA and Section 3.2 of the FSC Handbook, the Company must:

(a) identify, assess and understand the ML/TF risks for potential, new and existing clients/partners/stakeholders; business, products/services and systems may pose to the Company directly or indirectly
(b) Make an initial assessment of the risks to which it may be exposed through the (proposed) business relationship, (proposed) client relationship and verify the adequacy of its systems in place to review same regularly in accordance with the risks posed and change in circumstances
(c) Determine the appropriate level and type of mitigation to be applied, and
(d) Document and keep up to date risk assessments.

The Company shall avoid the “tick box” approach and consider the risk factors on a case-by-case basis.

The Board is responsible for managing the Company effectively and is in the best position to understand and evaluate all potential risks to the Company, including those of ML/TF. The Board takes ownership of, and responsibility for, the business risk assessments and ensure that they remain up to date and relevant.

Furthermore, the FSC expects that directors, officers and employees, irrespective of their level of seniority, must understand and accept their responsibility to contribute to the protection of the

financial institution against the risks of ML and TF, likewise all staff of the Company should be actively engaged in determining the risks posed by clients for ML/TF within those areas for which they have responsibility.

Refer to Appendix 5 for the detailed process of the Risk Assessment Policy.

4.5.2 RISK ASSESSMENT FRAMEWORK

A risk-based approach starts with the identification and assessment of the risk that has to be managed. A risk-based approach requires the Company to assess the risks of how it might be involved/used in ML/TF.

The Company has applied a risk-based approach comprising the following procedural steps to manage the ML/TF risks faced by it:

(a) Identifying the specific threats posed to the Company by ML/TF and those areas of the Company's business with the greatest vulnerability;
(b) Assessing the likelihood of those threats occurring and the potential impact of them on the Company;
(c) Mitigating the likelihood of occurrence of identified threats and the potential for damage to be caused, primarily through the application of appropriate and effective policies, procedures and controls;
(d) Managing the residual risks arising from the threats and vulnerabilities that the Company has been unable to mitigate; and
(e) Reviewing and monitoring those risks to identify whether there have been any changes in the threats posed to the Company which necessitate changes to its policies, procedures and controls.

The Company's Risk Assessment Framework shall comprise of the Business Risk Assessment, Customer Risk Assessment. The Customer Risk Assessment includes high countries risk assessment, controls and measures applied to mitigate the risks identified. To note that the Company shall not use any relevant AML/CFT Service Provider for CDD purposes.

A. CUSTOMER RISK ASSESSMENT

Chapter 5 of the FSC Handbook stipulates that "*Financial institutions must identify their customers, and where applicable, their beneficial owners and then verify their identities, which is essential to the prevention of money laundering and combatting the financing of terrorism. CDD is the means by which financial institutions achieve such knowledge and is a key element of any internal AML/CFT system*." Moreover, the risk-based approach is central to the effective implementation of the FATF Recommendations to combat Money Laundering and Terrorist Financing.

The Company will document a risk assessment for each customer in order to come to a risk rating of each customer in respect of the ML/TF risk. The risk rating exercise will not only be done at client acceptance stage but will be reviewed whenever there are changes in the investment plan or the profile of the client or changes in transactional trends occur. When the risk rating (as provided in the table below) is established and the client file must be reviewed in accordance with the risk rating attributed. Similarly, the frequency of screenings on each relevant party to any transaction must be conducted in accordance with the Risk Rating attributed, i.e. on a risk-based approach.

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

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

The Company has noted that being identified as carrying a higher ML/TF risk does not automatically mean that a customer is a money launderer or is financing terrorism/proliferation of weapons of mass destruction. Similarly, identifying a client as carrying a lower ML/TF risk of does not mean that the customer presents no risk at all.

In order to complete a meaningful risk assessment, it is recommended that information should be gathered prior to the assessment (this is the target although the Company is aware that this may not always be possible). A non-exhaustive list of these elements is provided below:

- The size, nature and complexity of the investment of the client
- The nature and type of client/partner/stakeholder
- The commercial rationale for the relationship
- The geographical location of the client /partner/stakeholder residence
- The geographical location of the client /partner/stakeholder business interests and / or assets (as may be applicable)
- The nature and value of the assets /funds concerned in the business relationship with any of its client
- The client/partner source of funds and wealth, as appropriate
- The role of any introducer and whether it is regulated or not
- The role and risks associated with any service provider and whether it is regulated or not

Upon completion of the risk assessment any additional information, evidence or clarification should be sought in the event that circumstances remain unclear, and the risk assessment should be updated accordingly. The total percentage attributed is then computed and the result is used to determine the level of risk of the client / business relationship.

After computing the risks in the CRA Questionnaire, the below table should be used to categorise the risk level of the client file / structure. Risk levels shall be classified into 3 categories:

Risk level	Risk Rating
Low	**0 – 59**
Medium	**60 – 129**
High*	**130 – 200**

The Company must be able to objectively and reasonably justify a risk assessment classification and document such justifications as well as mitigating and control applied to mitigate the identified risks and any decisions with respect to the review / adjustment / overriding of risk factor / assessment. The Company must adopt at all costs an unconventional approach when assessing the ML/TF risk associated with a client or category of customers in order to ascertain that all client risks aspects are effectively and duly captured.

The Company has devised a Customer Risk Assessment Questionnaire ('CRA'), as per Appendix 6B. The CRA is part of the Company's Risk Assessment Framework and will be a living document that shall be completed for each customer and shall be revisited and reviewed whenever new information is obtained about the customer.

The CRA will take into account the following risk factors:

- Customer Risk factors
- Products, Services and Transactions Risk factors
- Countries and Territories Risk factors
- Other Risk factors such as Technological developments and Delivery Channels

This exercise is undertaken through the completion of a series of successive stages of information gathering. The completion of each stage will inform the scope and structure of the following stage.

All CRAs shall be reviewed and signed off by the Compliance Officer or MLRO/DMLRO in line with the prevailing four-eyes principle.

A.1 Automatic High-Risk Ratings

Where a Politically Exposed Person (PEP) / Former PEP / Close Associate / Family Member to a PEP or a High-Risk Country has been identified prior to or during the business relationship, the client file shall be **automatically** categorized as **high risk**, EDD measures shall be applied in accordance with Regulation 12(1) of FIAML Regulations 2018 and Chapters 5 and 6 of the FSC Handbook, and approval of Senior Management or Board (as may be applicable) be sought to continue / start the business relationship.

A.2 Frequency for the conduct of the CRA & Risk-Based Monitoring

In order to ensure that the CRA remains up to date and to assess whether there are any changes in the risk profile of a client, amongst others, the CRA shall be reviewed on risk basis at the following frequencies:

Risk Level	Monitoring	Frequency of CRA, File Review & Screening
Low	Standard Due Diligence	36 months
Medium	Standard Due Diligence	24 months
High	Enhanced Due Diligence & Close Scrutiny of Transactions	12 months
• At the point of a material change in the Client's circumstances		
• Simplified Due Diligence shall be used on exceptional basis.		

It may happen that, upon the occurrence of a specific event or situation, it becomes obvious that the Risk Rating needs to be amended, that is, either increased or decreased. This change in Risk Rating shall be approved by the Compliance Officer or MLRO/DMLRO.

Each client file shall hold the individual questionnaire duly executed as part of the documentation and records relating to the client. The rating obtained will also be used to evaluate the business risk of the Company, as defined below.

For avoidance of doubt, clients of the Company include a prospective client, the existing clients of the Company and any of their principals but do not include consultants, persons giving loans to the client, subsidiaries, associates, investee companies or companies involved in joint venture projects, the beneficiaries, etc.

B. BUSINESS RISK ASSESSMENT

The Company has devised its Business Risk Assessment Questionnaire ('BRA'), as per Appendix 6A, which forms part of its Risk Assessment Framework. The BRA is designed to assist the Company in making an assessment and provide a method by which the Company can identify the extent to which its business, its services and relationships may be exposed to ML/TF. Business risk assessments are vital for ensuring that the Company's policies, procedures, and controls are proportionate and targeted appropriately.

The BRA will help the Company meet the requirement of recording and documenting its risk assessment as well as mitigating factors and control applied to mitigate the identified risks. The BRA shall be properly documented. Both Directors shall sign off the BRA which shall be approved at Board level.

Where the Company may have adjusted its risk assessment based upon information received after the establishment of a customer relationship and/or the use of the services of a relevant stakeholder/service provider, this should be well documented, along with the reasoning for such adjustment, and duly signed off.

Section 17(2) of the FIAMLA further requires the Company to assess 6 key areas when undertaking the business risk assessment:

(a) The nature, scale, and complexity of its activities;
(b) the client's risk;
(c) the products, services and transactions provided by the Company;
(d) nature, scale, complexity, and location of customer's activities;
(e) technological developments and delivery channels;
(f) reliance on third parties for elements of the customer due diligence process.

In conducting this BRA, the Company shall take into account the outcome of the risk assessment carried out at the national level and any guidance issued as required under section 17(2)(b) of the FIAMLA. As such, the report includes an assessment and evaluation of:

a. the adequacy of management information systems in place to deliver the information required by the senior management to ensure compliance with their responsibilities;
b. the Company operation and effectiveness of its anti-money laundering systems and controls;
c. appropriate coverage of new products and services, material changes in new customers take on procedures, impact of new regulatory changes in business profile;
d. the way in which new national and international findings have been used during the year.

The report shall also provide detail on:

a. documentation of risk management policies and risk profiles;
b. the risk mitigating measures contemplated;
c. risk monitoring arrangements to ensure that all areas adequately covered.

B.1 Frequency for the conduct of the BRA

The assessment must be regularly reviewed and kept up to date. The Company's BRA will be reviewed annually - unless there is a material change in circumstance during the course of the year which warrants a revision of the Company's BRA. All reviews of the BRA shall be documented and signed off to evidence that an appropriate review has taken place.

B.2 BRA Records Keeping

Clear documentation must be prepared and retained by the Company Secretary as part of the Board Papers to ascertain that the Board and Senior Management can demonstrate their compliance with the requirements of Section 17 of the FIAMLA at all times.

C. HIGH COUNTRIES RISK ASSESSMENT

When considering the geography risk factor, the following policy shall apply with respect to high-risk countries.

Section 17H (1) of the FIAMLA provides that where a jurisdiction is identified by the Financial Action Task Force ('FATF') as having significant or strategic deficiencies in its anti-money laundering and combatting the financing of terrorism and proliferation measures (AML/CFT measures), the Minister to whom responsibility for the subject of money laundering is assigned ('Minister') may, on the recommendation of the National Committee for Anti-Money Laundering and Combating the Financing of Terrorism ('National Committee'), identify that jurisdiction as a high-risk country.

On 21 October 2022, FATF issued the following statement: "High-Risk Jurisdictions subject to call for action". In the light of the jurisdictions identified by FATF in the statement, the Minister has on the recommendation of the National Committee, identified the following countries as high-risk countries:

- Democratic People's Republic of Korea
- Iran and;
- Myanmar.

(Source: General Notice No. 360 of 2023 of the Mauritius Government Gazette.)

The Company shall NOT onboard customers from a high-risk country as identified by the Minister.

It should be noted that the FATF statement "High-Risk Jurisdictions subject to a call for action" is different from the "FATF list of other monitored jurisdictions" as they are classified as high risk, but the FATF does not call for the application of enhanced due diligence to be applied to jurisdictions which are placed on the "Jurisdictions under Increased Monitoring" list. The FATF does, however, encourage its members to take into account the information presented on that jurisdiction in their risk analysis.

The Company shall consider such information from identified credible sources (e.g., FATF, EU, Transparency International) about countries and territories on issues relating to Money Laundering, Terrorism / Proliferation Financing, corruption, sanctions, and embargoes etc. when conducting its risk assessment.

The CRA takes into account various risk factors, including the geography risk factor (as specified under 4.5) and shall ensure that any one factor does not unduly influence its weighting. Therefore, even though a customer is from a country listed on the FATF list of other monitored jurisdictions and the

geography risk factor is high, other risk factors may be rated as low and when all risk factors (as specified under 4.5) are considered collectively, the customer's risk rating may be low or medium risk.

D. POLITICALLY EXPOSED PERSONS ("PEPS")

PEPs are individuals who are and who have been entrusted with prominent public functions (for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations and important political party officials). The definition of PEP includes foreign, domestic and international organisation PEP, as well as the close relatives and associates of such persons.

It is noted that relationships with PEPs, family members or close associates of PEPs are deemed to pose a greater than normal money laundering risk by virtue of the potential for them to have benefited from proceeds of corruption as well as the potential for them (due to their offices and connections) to conceal the proceeds of corruption or other crimes.

The Company shall ascertain whether any controlling person within the structure of an existing customer or with connected persons are PEPs / Former PEPs or becomes a PEP or close associate of a PEP during the client relationship through its file reviews and monitoring of the client relationship. As stipulated in the FSC Handbook, "connected persons" will include underlying principals such as beneficial owners and controllers. The Company will be able to determine the foregoing through the screening carried out on clients as per section 5.5. All such clients' details shall be duly recorded in the PEP Register maintained by the Company's MC.

The EDD measures referred to under section 5.3.3 shall apply accordingly and an entry shall be made in the register of PEPs.

There is a view or regulatory approach of Know Your Customer ('KYC') that "*once a PEP, always a PEP*" which the Company shall apply. Hence, any controlling or connected person, formerly a PEP or a relative or close associate of a PEP, who is no longer entrusted with a prominent public function ("Former PEP") or the Former PEP's family members or close associates will still be subject to the EDD measures on a risk-based approach.

4.5.3 TRAINING

Regulation 22(1)(c) of FIAML Regulations 2018 states that programmes against ML/TF should be in place. The Company is committed to the annual and ongoing periodic training and development of its board members, officers, and employees. Regular training ensures that all staff stay aware of their responsibilities in respect of prevention of money laundering including the application of adequate controls, understanding what might constitute suspicious behaviour and how to report an such suspicions. Training also includes informal training courses, communication that serves to educate and inform employees such as emails, newsletters, guidance notes, periodic team meetings and anything else that facilitates the sharing of information.

There should be a minimum of at least one AML/CFT training session annually.

Besides the above, the Compliance Officer / MLRO, Deputy MLRO, Directors, Officers, Investment Dealer Team will follow external structured CPD points trainings, in line with the requirements under the FSC Competency Standards while the members of the Investment Dealer Team should also be trained in Investment Dealing matters (in line with their roles in the Company, wherever required).

The Compliance Function will be responsible for providing organisational assistance in this regard, and for ensuring that training is implemented and documented in the Training Register.

5.0 CLIENT IDENTIFICATION AND VERIFICATION PROCEDURES

5.1 CUSTOMER DUE DILIGENCE ('CDD') POLICIES AND PROCEDURES

Client identification and verification facilitates the prevention, detection, and prosecution of the illegal use of the securities sector. Effective client identification and verification procedures are necessary to protect the Company, its customers and to maintain the integrity of the securities markets.

Customer and beneficial owner identification and verification, Know Your Customer ('KYC'), as well as the keeping of the related data are considered the Client Due Diligence process ('CDD process'). The CDD process is a key component of securities regulatory requirements intended to achieve the principal objectives of securities regulation, the protection of investors/clients, ensuring that markets are fair, efficient, and transparent and the prevention of the illegal use of the securities industry.

In addition, to reduce the risk of exposure to ML/TF, effective CDD practices also protect the Company against a range of other potentially damaging risks including reputational risk, legal risk and the risk of regulatory sanction. The Company shall adhere to FIAMLA, and FIAMLR and refer to the guidance provided by the FSC Handbook on CDD requirements.

5.2 RESPONSIBILITY FOR CLIENT IDENTIFICATION AND VERIFICATION AND CLIENT ON-BOARDING

Investor/traders/clients furnishes at least POI and POA following which the Company verify these documents. The Management Company shall counter check these CDD documents and once approved – the client is allowed to trade. No client can trade without approval of CDD documents.

The CDD process shall be carried out by the Management Company in accordance with this Compliance Manual to fulfil the customer and beneficial owner identification and verification requirements.

The Management Company has been delegated the responsibility to maintain records of the identification information and documentation and the verification of documentations that the Company has obtained through the CDD process. The process is as follows:

- Prior to onboarding a client, the Backoffice team / Onboarding Team of the Company ensure that their KYCs (certified wherever necessary – section 5.12 of this Manual refers) are collected and screenings are conducted.
- The clients are onboarded after successful registration.
- The Company then share the documents with the Management Company. Depending on the volume – daily, weekly, or monthly; The latter conducts a second review of the KYCs and screenings.
- The client is then risk rated and same is revisited on a periodic basis depending on weightage.

- In case, any adverse matches are triggered, the Management Company notifies the Company for either;
    i. Additional Documentation
    ii. In case of PEP – the declaration form and enhanced supporting documents.

- If the client is not cooperative – the account is suspended. Depending on the response – the account will ultimately be closed, and funds will be remitted as applicable to the source.

- The above is treated on a case-to-case basis and a Risk-Based Approach is applied.

- The seriousness and/or likelihood of the adverse match is evaluated.

Migration of Investors/Traders/Clients

For any migration of clients, the migration process as per Section 6.2.3 shall be applicable.

Trading without complete CDD

Where the KYC process is incomplete, the account of the client is put on hold until same is completed. Once the account is fully verified, that is, a valid POI and a recent POA have been received – the client will be eligible to start depositing and trading.

5.3 HOW SHOULD THE IDENTITY OF CUSTOMERS BE VERIFIED?

The Management Company which has been assigned the responsibility of carrying out the CDD process of the Company shall follow a risk-based approach to CDD. The customer risk levels (High, Medium, Low) obtained pursuant to section 4.5 (A.2) will help determine the extent and frequency of CDD information and documents that will be requested on a customer. Please refer to the client onboarding process of the Company. See Appendix 11 for updated CDD Documents guidelines.

The company has adopted standard customer due diligence procedures and a risk-based approach based on international best practices.

5.3.1 SIMPLIFIED CDD MEASURES

Simplified or reduced CDD measures may be applied on exceptional basis.

The rationale for the decision to apply simplified CDD should be documented appropriately by the Compliance Officer / MLRO / DMLRO, i.e., in a manner which explains the factors which he / she took into account (including retaining any relevant supporting documentation) and its reasons for adopting the measures in question. Similarly, any change in the measures adopted shall be equally documented. That's said, situations which present high risk cannot and must not be over-ruled.

The Compliance Officer / MLRO / DMLRO shall review the relationship with the customer (including the appropriateness of applying / maintaining simplified measures) at such frequency as required under section 4.5.

5.3.2 STANDARD CDD MEASURES

Standard CDD measures will be applied where lower and medium risks have been identified. Standard CDD measures shall include:

(a) The identification and verification of the identity of each customer;

(b) The identification and verification the identity of individuals connected to the customer such as the customer's beneficial owner(s) or related to any transaction;

(c) Obtaining information on the purpose and intended nature of the business relationship;

(d) The conduct of ongoing due diligence on the business relationship and scrutiny of transactions throughout the course of that relationship, to ensure that the transactions in which the customer is engaged are consistent with the Company's knowledge of the customer and its business and risk profile (including the source of funds);

(e) The use of reliable, independently sourced documents, data, or information (e.g., commercial databases and public information) to sustain the above;

(f) All material collected under the CDD process is kept relevant and up to date.

5.3.3 ENHANCED CDD MEASURES

The Company shall apply the EDD measures in accordance with Regulation 12(1) of FIAMLR as follows:

1. Where a higher risk of ML or TF has been identified;
2. Where through supervisory guidance a high risk of ML or TF has been identified;
3. Where a customer or an applicant for business is from a high risk third country;
4. In relation to correspondent banking relationships, pursuant to Regulation 16 of FIAMLR;
5. Subject to Regulation 15 of FIAMLR, where the client or its principals or the applicant for business is a PEP, family members or close associates of PEPs;
6. 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;
7. In the event of any unusual or suspicious activity;
8. In case the financial history or background of the end-client cannot be ascertained;

The Management Company has been assigned the responsibility to carry out EDD measures on behalf of the Company.

A. PEPs Due Diligence Procedures

Similarly, the Company shall apply EDD measures when dealing with PEPs or close Associates of PEPs in accordance with Regulation 15(1) of the FIAMLR which provides that the following measures must be established with respect to dealings with PEPs:

- Put in place and maintain appropriate risk management systems to determine whether the customer or beneficial owner is a PEP;
- Obtain senior management approval before establishing or continuing, for existing customers, such business relationships;
- Take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPs.

B. HIGH RISK COUNTRIES

The Company is required to apply enhanced due diligence (EDD) measures with respect to persons from a high-risk country. Section 17H of FIAMLA provides that where a jurisdiction is identified by the Financial Action Task Force as having significant or strategic deficiencies in its AML/CFT measures, the relevant Minister may, on the recommendation of the National Committee and after giving due consideration to such factors as may be prescribed, identify that jurisdiction as a high-risk country.

The Company shall make a distinction between high-risk countries as identified by the Minister under section 17H of FIAMLA and countries identified by the FATF as having strategic AML/CFT deficiencies and having not made sufficient progress in addressing those deficiencies.

Notwithstanding the provisions of section 17H of FIAMLA, the Company shall **NOT** accept any clients from or accept to invest into or transfer any funds/assets to such high-risk country as identified by the Minister under section 17H of FIAMLA. On the other hand, the Company shall apply Enhanced CDD in accordance with item 2 of the EDD Cases below for client relationships and transactions with any person from countries identified by the FATF as having strategic AML/CFT deficiencies and have not made sufficient progress in addressing those deficiencies.

C. OTHER EDD CASES

To sum up, the Company will adopt enhanced due diligence measures in the following cases:

	CASES	EDD MEASURES
1.	The client is classified as High Risk under the Risk Assessment Policy.	Enhanced due diligence measures in accordance with section 5.3.3 on the basis of the client's risk rating will be put in place to monitor the client.
2.	Where High Risk Countries or Non-Cooperative Countries or Territories ("NCCT") (as issued by the FATF) or countries which have been subject of FATF Public Statements for deficiencies in their AML / CFT systems are involved or EU high risk countries.	Enhanced due diligence measures in accordance with section 5.3.3 on the basis of the client's risk rating will be put in place to monitor the client.
3.	The client (i.e. the shareholder, beneficial owner* or family member or authorised signatory or any of its controlling persons (where the client is a body corporate) is a former Politically Exposed Person (PEP) or former close associate of a PEP. (Refer to section 5.3.3.A)	Approval of Client Acceptance Committee shall be required. Due consideration shall be given to: a. Any adverse publicity that the Former PEP may have been involved in corruption, money laundering, bribery, fraud, terrorist financing; b. The source of funds/wealth of the client; c. The profile of the entities or persons related to the client; d. The level of (informal) influence that the individual identified as PEP could still exercise on the account; e. The seniority of the position the individual held as a PEP within the account where the latter is held through a body corporate; f. Whether the individual's previous and current function are linked in any way. The following shall apply: (i) An entry shall be made in the register of PEPs specifying clearly that client is classified as Former PEP. (ii) The overall risk level shall automatically be reclassified as High Risk unless the findings (a) to (f) above demonstrate otherwise. The rating where there is a

		Former PEP shall not be inferior to high risk. (iii) Enhanced due diligence measures in accordance with section 5.3.3.A on the basis of the client's risk level shall have to be applied.
4.	Where during the course of a client relationship, it is found that a customer has provided false or stolen identification documentation or information	The Company has to terminate the client relationship: (i) File an internal STR to the MLRO, as may be applicable, and an external STR to the FIU in accordance with section 14 of the FIAMLA (ii) Inform the client of the termination of the client relationship without tipping off (see sections 5.3.3 in this regard)
5.	In the event of any unusual or suspicious activity.	▪ Measures under sections 5.3.3 shall apply

**Beneficial owner shall mean a natural person who ultimately owns or on whose behalf a transaction is being conducted or who controls a customer Controller as defined under section 2 of the Financial Services Act 2007, that is, a controller in relation to a corporation, means a person:*

(a) who is a member of the governing body of the corporation;
(b) who has the power to appoint or remove a member of the governing body of the corporation;
(c) whose consent is needed for the appointment of a person to be a member of the governing body of the corporation;
(d) who, either by himself or through one or more other persons –
(i) is able to control, or exert significant influence over, the business or financial operations of the corporation whether directly or indirectly;
(ii) holds or controls not less than 20 percent of the shares of the corporation;
(iii) has the power to control not less than 20 percent of the voting power in the corporation;
(iv) holds rights in relation to the corporation that, if exercised, would result in paragraphs (ii) and (iii);
(e) who is a parent undertaking of that corporation, or a controller of such parent undertaking;
(f) who is a beneficial owner or ultimate beneficial owner of the persons specified in paragraphs (a) to (e) and who appears to the FSC to be a controller of that corporation.

Where the Company is unable to satisfactorily apply enhanced due diligence measures as per its internal procedures, it shall terminate the business relationship with the client and where applicable, file a suspicious transaction report in accordance with section 14 of FIAMLA.

THIRD PARTY RELIANCE

5.4.1 KYC & CDD MEASURES

The CDD process is carried out by the Compliance Analyst dedicated to the Company, under the supervision of the Compliance Officer. Any request for missing document or information is escalated to the Operations team, who ultimately liaise with the end-Clients for same.

KYC and CDD measures, duties and functions will not be outsourced to any third party.

5.4.2 THIRD-PARTY SERVICE-PROVIDERS

It aims to establish standards and guidance relating to Company's management of its third-party relationships and the associated inherent and residual risks presented by those third-party relationships. These risks are present when the Company engages with third parties to provide products and services directly to the Company for the benefit of its internal operations, employees, investors, or customers.

Failure to manage these risks can expose the Company to financial loss, litigation, or other damages or may even impair the Company's ability to service existing customer relationships or establish new ones.

Prior to entering into an agreement, it is important to conduct due diligence of a Third Party. A Simplified CDD Measures or Standard CDD Measures shall be carried out by the Administrator dedicated to the Company. Any request for missing document or information is escalated to the Accounting Team, who ultimately liaise with the third-party service providers engaged in the operations.

Screenings and Third-Party Risk Assessment on the Service Providers shall be carried out by the Compliance Analyst dedicated to the Company. Please refer to Appendix 16.

- In case, any adverse matches are triggered, the seriousness and/or likelihood of the adverse match is evaluated. Accordingly, the followings will be requested:
    - Declaration of PEP Status Form (as applicable);
    - Clarification letter or any equivalent document with respect to the adverse matches.
- The service providers shall be onboarded after clean screenings.
- The frequency of the ongoing monitoring (screening & risk assessment) of the service providers shall be on a risk-based approach. For example, low risk will be reviewed every 3 years, medium risk will be reviewed every 2 years and high risk will be reviewed every year.

5.5 SCREENINGS

The Company will complement its CDD measures by conducting screenings on the Clients and on the controlling persons and connected persons of the institutional customers through independent searches using internationally recognized screening engines which already encompass the UN, OFAC, UK HMT, EU, DFAT Sanctions lists (just to name the salient ones) and publicly available information on the Internet.

The Management Company ensures that the screening engine being used in-house enables the flagging of any arising hit or adverse report as and when it appears on the global databases upon which search engine relies.

The Management Company must also ascertain that the screening includes searches against domestic and the United Nations Security Council List of Targeted Financial Sanctions. The Management Company must test the search engine with designated names received from the FIU / National Sanctions Secretariat / FSC, as may be applicable, and confirm to the Company that those names are duly captured.

Although the Company adopts a Risk Based approach, ongoing monitoring is conducted, including on low and medium risk customers, which goes beyond the risk-based approach adopted by the Company. These screenings shall help the Company to ensure that there are no sanctions or other hits / adverse media reports on the customer relating to financial fraud or crime, financial threat, tax evasion, drug trafficking, organized crime, matters relating to money laundering and financing of terrorism / proliferation ("Adverse Media").

The procedures under Appendix 10 shall be followed where Sanctions / Adverse Media have been found.

- The Management Company has put into place the software, namely Refinitiv as well as 24/7 screening tool called Infinitix. This software is used for main Principals of the Company and its end clients. In case there is any change in the status of the main Principal or the end clients, such as PEP or adverse matches, a notification will trigger, and the Management Company will ensure that additional documents are requested and held on file.

5.5.1 RISK BASED APPROACH TO SCREENING

The FIAMLR and the FSC Handbook require that screenings must be conducted regularly on a risk basis as warranted under a risk-based approach.

Screenings for the Principals / Officers of the Company are conducted on a periodic basis.

Screenings for the Clients of the Company are conducted at the time of onboarding. Given the Client Risk Assessment level (clients that are rated as low, medium, or high-risk clients), screenings on the clients shall be conducted annually for high risk level, every 2 years for medium risk level and every 3 years for low risk level.

Should there be a trigger event for a particular Client (e.g., PEP, high risk countries or high volume of investments), re-screening is conducted. If any suspicious activities are identified, a Suspicious Transaction Report ("STR") procedure is initiated.

5.5.2 SANCTIONS SCREENING

a. Sanction screening is to ensure compliance with the applicable sanctions against persons and entities that the Company has put in place to compare the entity name, beneficial owners, directors and authorised persons with official list of;

   1. The US Department of the Treasury Office of Foreign Assets Control
   2. (OFAC) sanctions list; https://sanctionssearch.ofac.treas.gov/
   3. The UK HM Treasury (HMT), office of Financial Sanctions implementation, "consolidated list of targets";
   4. https://ofsistorage.blob.core.windows.net/publishlive/ConList.html
   5. The United Nations (UN) Security Council consolidated sanctions list; https://scsanctions.un.org/search/ https://scsanctions.un.org/consolidated/
   6. Financial Action task force, Member countries;
   7. All other applicable sanctions laws and regulations in the Mauritius jurisdiction; and
   8. IBAN Check for screening of Shell Banks. No business relationship is established if customer presents shell Banks details for account application. https://www.iban.com/

b. In line with the above, whereby a potential match is identified, Enhanced Due Diligence ("EDD") will be applied in order to determine whether the match correspond to our clients. Further to the additional documents / information submitted, the following actions will be taken:

   - If the potential match is positive, that **is related** to the client, immediate action will be taken by the Compliance Officer to terminate the business relationship.

   - If the potential match is negative, that is **not related** to the client, the Compliance Officer will update the Register of False Positive Matches.

c. To conclude, all potential sanctioned entity or individual is investigated, and relationship is terminated if the match relates to the client.

5.5.3 TARGETED FINANCIAL SANCTIONS

5.5.3.1 REPORTING OBLIGATIONS AND PROCEDURES

The Company is required, under Section 41 of the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Act 2019, to implement internal controls and other procedures to effectively comply with the obligations of the Act. The Guidelines on the implementation of Targeted Financial Sanctions further provides for sanctions screening.

The MLRO shall regularly consult the United Nations Security Council Consolidated List and take immediate action with respect to any changes brought thereto. The MLRO will also regularly consult the newspapers for any notice which may be issued by the National Sanctions Secretariat and immediately act upon it.

Customer screening includes the screening of the directors, beneficial owners, and other related parties with access to the account. In addition, sanction screening must be conducted in the following events:

1. When there is a trigger event, that is, change in the customer information, such as change in shareholding information, the appointment or re-appointment of new controlling persons;

2. When there is a change in the sanctions list or update in the sanction's regime.

5.5.3.2 SANCTIONS REPORTS

- The Company has devised appropriate measures in place for the screening and verifications of its clients to identify designated persons under the UN or targeted financial sanctions list; https://scsanctions.un.org/consolidated/

- If a POSITIVE match is identified by a reporting person, a report must be submitted to the National Sanctions Secretariat regardless of whether funds/assets have been identified or not. In some cases, a similar report must also be submitted to its relevant supervisory authority. The specific reporting obligations contained in the UN Sanctions Act should be taken into consideration.

- Upon receipt of the Sanctions lists from the concerned Authorities, the Clients' database is checked and accordingly, no reports will be submitted to the National Sanctions Secretariat, unless a positive match is triggered on any specific client. However, sanctions screening register will be updated internally, and evidence of the sanction screenings will be kept on records.

- Reports may be completed using the template which can be downloaded from the NSSEC website: http://nssec.govmu.org

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

Relevant obligation in UN Sanctions Act	Description	Sanctions for noncompliance
Section 23(4)- Notification of compliance with	Details of any funds or other assets subject to a prohibition to deal under section 23(1) of the Act must be immediately reported to the National Sanctions	Failure to comply with this requirement is an offence under

prohibition to deal requirement	Secretariat in terms of section 23(4) of the UN Sanctions Act. The report must provide- a) Details of the funds or other assets against which action was taken in accordance with section 23(1) of the UN Sanctions Act; b) The name and address of the listed party; c) Details of any attempted transaction involving the funds or other assets, including – o The name and address of the sender o The name and address of the intended recipient o The purpose of the attempted transaction o The origin of the funds or other assets o Where the funds or other assets were intended to be sent	section 45 of the UN Sanctions Act.

5.6 SOURCE OF FUNDS / SOURCE OF WEALTH

In the identification of ML/TF risk, it is a pre-requisite to understand the source of funds and / or source of wealth (as may be applicable), in relation to the intended business activity of the client.

Source of funds is the origin of the particular funds or assets which are the subject of the business relationship between the Company and the client and the transactions the Company is required to undertake on the customer's behalf (e.g. the amounts being invested, deposited or remitted) while the source of wealth is distinct from source of funds and describes the origins of a client's financial standing or total net worth, i.e. those activities which have generated a client's funds and property.

The Compliance Analyst, under the supervision of the Compliance Officer, takes appropriate measures to verify the source of funds and / or source of wealth (as may be applicable) for each applicant for business on a case-by-case basis.

- Pursuant to Section 5.3.3, ''EDD Measures'', the clients will be requested to complete and sign a declaration of source of funds and wealth (Appendix 13) and submit relevant supporting documents as evidence of source of funds;

- Where, the above is not applicable, the clients shall provide their declaration of the source of funds and wealth on the application form (see 5.7.1 below);

- Ensure there is consistency between the information on the customer, source/evidence of funds and intended business activity.

In case of any inconsistencies, additional measures to verify the information obtained / seek clarification and consider obtaining information regarding the customer's source of wealth will be taken.

A customer may be exempted from providing supporting documents to evidence the source of funds in the following cases:

- Client's profile is publicly available (e.g. Forbes lists) and demonstrates that he / she is clearly wealthy from legitimate means to justify the source of the funds.

- Source of funds originates from an established business of the shareholder / beneficial owner and the financial statements of the shareholder / beneficial owner demonstrate that the funds being injected are available.

- Client is injecting an amount already held/administered by a regulated financial institution duly licensed in an equivalent jurisdiction and the client has provided a (bank) statement showing an excess of that amount on his/her (bank) account.

- Injection (by way of equity, loan, advances etc.) of funds from another investment account which is already under administration of the Company provided that the source of funds of the other account had already been satisfactorily established.

- Client's profile or status (inheritance for instance following the demise of parent or spouse, or past track record, etc.) is publicly available (e.g. Forbes lists or independent media) and demonstrates that he / she is clearly wealthy from legitimate means to justify the source of the funds injected in the client account to be managed by the Company.

The above list is non-exhaustive but reflects the philosophy of the Company in ascertaining independently and reliably the source of funds /wealth of any client. In any case, the decision to exempt the client from submission of evidence of source of fund must be documented and justified on file.

5.7 ONGOING MONITORING OF EXISTING CLIENTS

This implies:

(a) Screening of clients (Refinitiv and Infinitix – a new software which has just been acquired by the MC) to be done by the MC on behalf of the Company;

(b) Handling of Adverse Media / compliance reports in accordance with Appendix 10;

(c) Verifying source of funds / wealth, where applicable;

(d) Ensuring that documents, data, or information collected are kept up to date and relevant by undertaking reviews of existing records as per Appendix 11;

(e) Obtaining information on the reasons for intended or performed transactions / scrutiny of transactions undertaken throughout the course of the relationship, by way of review of bank statements or otherwise, to ensure that the transactions are consistent with its knowledge of the customer and the business and risk profile of the customer;

(f) obtaining the approval of the Board to continue the business relationship;

(g) Reviewing the risk assessments of the customers on a risk basis.

Where the Company is unable to satisfactorily apply enhanced due diligence measures as per its internal procedures or where the Company has discovered that the customer has provided false or stolen identification documentation or information, it shall terminate the business relationship with the customer and where applicable, file a suspicious transaction report as required. The Company shall adopt its Internal Procedures Manual which elaborates on Internal and External Reporting Procedures in this regard.

5.7.1 TRANSACTION MONITORING

The Company shall conduct the CDD process from the moment a business relationship is established and on an ongoing basis thereafter.

The Company will provide the following services, namely:

- manage, under a mandate, portfolios of securities for its clients.

Since the Company will manage the portfolios of securities for its clients, no further scrutiny of transactions shall be required to ensure that the transactions are consistent with the knowledge and the business and risk profile of the client.

However, the Company shall ensure that the source of any inflow of funds / funds to be used for acquisition of securities is verified / established. A declaration of source of funds (Appendix 13) shall be completed in this respect. Please refer to Section 5.3.3 on Enhanced Due Diligence Measures.

Please also refer to Section 3.5 on Transaction Monitoring in this regard.

A. REAL TIME TRANSACTION MONITORING

The company will ensure that the KYC documents received from the clients are valid. The company will adopt the practice of Standard Customer Due Diligence for this process.

Any deposit or withdrawal made by the clients either by local bank / foreign bank or Payment Service Provider as applicable – the real time monitoring is carried out by the Operations Team / Dealing Team of the Investment Dealer.

The Management Company of the Company shall conduct the transaction monitoring on a fortnightly basis. Depending on the volume of transactions (high or low), the frequency of TM will therefore be daily, weekly, monthly, or quarterly. The Management Company shall request either daily or weekly transaction reports and monitoring will be conducted.

As part of the transaction monitoring, additional documents (EDD) will be requested where applicable. The Declaration of Source of Funds / Source of Wealth shall be completed by clients who meet the Enhanced CDD criteria as identified in section 5.3.3 and/or for the clients who does not falls in the criteria of EDD measure then, they will complete this declaration on their application form (as applicable).

B. POST TRANSACTION MONITORING

Thereafter depending on the volume of transactions, the Management Company requests on an either daily, weekly, or monthly basis for a second verification.

The above is documented and monitored.

For the view access, Credentia always emphasises on the need to have the view access for the local director, however, the banking system of the foreign bank is not the same as for the Mauritius local banks.

5.7.2 REGULAR MONITORING

The Company will periodically review the adequacy of client identification information obtained in respect of customers and ensure that the information is kept up to date. In this respect, the MLRO / DMLRO / Compliance Officer shall conduct the following monitoring of clients shall be carried out at the determined frequencies:

Monitoring				
Risk level	**Verifying source of funds**	**Updating CDD documents**	**Screening**	**Review of client risk assessment**
Low risk	Upon onboarding and new transactions	As per Appendix 11	Although a low-risk client, the Company applies enhanced screening measures by conducting screenings	Every 3 years; or in the event of a material change in the client's circumstances, whichever the earlier.
Medium risk	Upon onboarding and new transactions	As per Appendix 11	Although a medium risk client, the Company applies enhanced screening measures by conducting screenings	Every 2 years; or in the event of a material change in the client's circumstances, whichever the earlier.

High	Upon onboarding and new transactions	As per Appendix 11	Although a high risk client, the Company applies enhanced screening measures by conducting screenings	Yearly; or in the event of a material change in the client's circumstances, whichever the earlier.

Same as section 5.5 - ''the Company shall opt for Infinitix as a screening tool for its end clients. Simultaneously, in case there is any change in the status of the clients, that is one of them has become a PEP or adverse media has been noted, a notification will trigger, and the Management Company will ensure that additional documents are requested and held on file.''

Funds redeemed or withdrawn are transferred to the Client at source, that is if the Client has deposited through Credit Card, the funds will be returned to the same Credit Card details.

5.7.3 FOUR EYES PRINCIPLE

The Four Eyes Principle (also called 'Dual Control') forms part of the Internal Control Mechanism of the Company and requires that any activity within the organization that involves material risk profile must be controlled, i.e. reviewed / double checked by a second competent individual.

The objective of the control is to mitigate risks primarily of the following two types:

- Business Execution - adverse outcomes as the result of poor execution of regular business tasks (mistakes, oversights);

- Internal Fraud - adverse outcomes as the result of fraudulent action of persons internal to the firm.

The "four eyes" principle can be implemented in different ways to allow for double check and control and efficient monitoring in terms of assessment of risks, transactions amongst others.

The overriding requirement is for the four eyes (at least two individuals) criterion to be met on a continual basis over the entire operations or certain types of operations which usually would pose more risks to the Company.

Therefore, every existing or new procedures of the Company have to be implemented in such a manner that the "four eyes" principle is respected accordingly.

5.8 INTERNAL AND EXTERNAL REPORTING PROCEDURES

The Company shall adopt the Internal Procedures Manual which elaborates on Internal and External Reporting Procedures with respect to Reporting of Listed Parties and Suspicious Transactions.

The MLRO / DMLRO will devise and maintain the following logs for the Company pertaining to reporting under this section.

- A Log of Internal Reports of suspicious transactions / activities filed with the MLRO/DMLRO
- A Log of External Reports of suspicious transactions / activities filed with the FIU by the MLRO/DMLRO
- A Log of Reporting on Positive Name Match under section 25(2) of the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019
- A Log for Notifications to the National Sanctions Secretariat and to the FSC under section 23(4) of the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019
- A Log of Rejected Clients

5.8.1 REPORTING OF SUSPICIOUS TRANSACTIONS

5..8.1.1 TRANSACTION SCREENING AND MONITORING:

The Company will do ongoing transaction monitoring and sanction screening of all clients, single transaction monitoring and risk assessment, profiling, and clients' transactional behaviours. The alerts generated upon verification by Compliance Officer, EDD will be applied and appropriate actions in case of suspicion.

In general terms, the concerned Staffs should have regard to the following considerations when monitoring client accounts, as well as other factors detailed in other chapters of this Manual:

- The unusual nature of a transaction: e.g., abnormal size or frequency for that client or type of client.
- The nature of a series of transactions: for example, a number of cash credits.
- The geographic destination or origin of a funding payment: for example, from a high-risk jurisdiction.

The Company recognises that client behaviour may vary widely, therefore making it harder to pick up unusual or suspicious trading activity. Also, because the Company does not provide advice to clients and does not own suitability obligations to them, we will hold little information about their trading motives. When the Company opens a client account on a non-face-to-face basis, and the payment is proposed to be made from an overseas account, the Company will seek to mitigate this risk by establishing that the overseas account is held in the client's own name. If we are unable to establish this, we will review the account and transaction history; and enquire of the reason for making the payment abroad. This way we will seek to determine whether the account, or any dealings on it, are unusual, and therefore possibly suspicious.

The trading team monitors client trading activity, including electronic fund transfers on an ongoing basis. Staff are trained to identify "triggers" requiring follow up due diligence. For example, disconnected telephone numbers or returned mail would trigger a client account's suspension until the KYC information

is updated. Staff are trained to identify and verify beneficial ownership information for all non-individual customer types on an ongoing basis.

Where beneficial owner or true controllers are determined, additional KYC information is collected and verified. On a case by case basis, the Compliance Analyst dedicated to the Company's files, monitors transactions of customers, including complex or unusually large transactions and odd patterns of transactions which have no apparent economic or visible lawful purpose.

On a case by case basis, staff on the account opening team manually monitor client accounts for suspicious activity. Client accounts are monitored by staff on an ongoing basis in order to identify any suspicious activity. Staff review deposits and trading activity to ensure transactions comply with AML/CFT policies. Suspicious patterns trigger an escalation procedure and are reported to the team's line manager who will notify Compliance and an investigation will pursue.

5.8.1.2 iSTR

An Internal Suspicious Transactions Report (iSTR) is raised by the officer, employees, or operations team (the Company's team members), to the MLRO in case of any suspicion that has come to their attention. All the iSTR are logged with the relevant supporting documents/evidence of suspicion.

The Company has designed an iSTR form (Appendix 9), which every team member of the Company can use to report the MLRO for any suspicion. The Company's team members can also inform the MLRO about any suspicion by phone or email.

The key indicators/red flags of suspicious activities include reasonable ground of suspicion that any service or transactions may be:

a. related to criminal conduct;
b. related to the laundering of money or the proceeds of any crime;
c. funds linked or related to, or to be used for, terrorist financing or by proscribed organisations, whether or not the funds represent the proceeds of crime; or
d. made in circumstances of unusual or unjustified complexity;
e. appear to have no economic justification or lawful objective; and
f. give rise to suspicion as per Section 5 of Guidance Note 3 issued by FIU (Specific Examples of Indicators of Suspicious Transactions).

5.8.1.3 STR

The Company has implemented the control of the Customer profiling and transactional monitoring; therefore, any possible alerts are reported to MLRO.

Under the FIAML Act 2002, the Suspicious Transaction Report (STR) means 'a transaction which:

a. Gives rise to a reasonable suspicion that it may involve:

1. The laundering of money or the proceeds of any crime; or
2. Funds linked or related to, or to be used for, terrorist 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; or
e. gives rise to suspicion for any other reason.

All the suspicious cases which are reported through iSTR, or identified independently from the MLRO, are reviewed and investigated in depth, taking into consideration the provisions of the FIAMLA and FIAML Regulations 2018, and any evidenced suspicion is reported by the MLRO to the FIU in prescribed from of STR as given in: http://www.fiumauritius.org/English/Reporting/Pages/default.aspx

Freezing of Assets

Where a Client is declared as a designated party or listed as a listed party under the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019, the Company will immediately, verify the details of the designated party or listed party, and also identify whether the Client owns any funds or other assets in Mauritius.

After identification of the Assets, the Company will make a report to the National Sanctions Secretariat as obligated, and any other Local Authority or Regulator as applicable.

Further to the proclamation of the Anti-Money Laundering and Combating the Financing of Terrorism (Miscellaneous Provisions) Act 2020, emphasis has been put on the obligation to report suspicious transactions, causing amongst others, the FIAMLA 2002 to be amended. The MLRO or the Deputy MLRO shall make a validated Suspicious Transaction Report (STR) 5 working days from the date on which the suspicion was raised.

Regarding the financial sanctions to the qualifying offences under FIAMLA shall upon conviction be as follows:

- Failure to report a suspicious transaction not later than 5 working days from the date the suspicion was rose – A fine not exceeding MUR 1 million and a term of imprisonment not exceeding 5 years;
- Failure to apply an effective risk assessment in view of detecting an act of money laundering and terrorism financing – A fine not exceeding MUR 10 million and a term of imprisonment not exceeding 5 years;
- Conspiring or assisting in a claimed financial malpractice – A fine not exceeding MUR 10 million and a term of imprisonment not exceeding 5 years;
- Causing obstruction by destroying evidence and relevant records – A fine not exceeding MUR 10 million and a term of imprisonment not exceeding 5 years;

- Objection or failure to provide such requested information to the regulatory body – A fine not exceeding MUR 1 million and a term of imprisonment not exceeding 5 years.

5.8.1.4 TIPPING-OFF

a. Tipping off is prohibited under the provision of Section 19 (1)(c) of the FIAMLA 2002;
b. Since it is an offence based, the MLRO ensures that the management and employees are aware of and are sensitive to the data sharing, and consequences of tipping off;
c. In case the officer and/or employee believes, or has reasonable grounds to believe, that a Client may be tipped off by conducting CDD measures or on-going monitoring, the employee should refer the case to MLRO. The MLRO shall maintain records to demonstrate the grounds for belief that conducting CDD measures or ongoing monitoring would have tipped off the Client;
d. If an internal STR is sent to the MLRO, the employee should not disclose this to the Client or any other person;
e. The MLRO should not accord permission or consent to disclosure of information relating to internal STR to any person, unless MLRO is satisfied that such disclosure would not constitute tipping off;
f. Any letters, notices, or requests received from FIU, or Police these should not be disclosed to any person outside the Compliance Team or Client;
g. The only permitted exception, apart from disclosures to the FIU and Police, are disclosures to;
    1. an officer or employee or agent of the reporting entity for any purposes connected with the performance of that person's duties;
    2. a legal practitioner, attorney, or legal adviser for the purpose of obtaining legal advice or representation in relation to the matter; and
    3. the supervisory authority of the reporting entity for the purpose of carrying out the supervisory authority's functions.
h. The MLRO should ensure that all officers and employees need to understand that they could be personally liable for non-compliance with the AML obligations; and
i. The MLRO is the person responsible for relevant training in identifying AML suspicious transaction for all officers and employees.

5.8.1.5 RECORDS OF SUSPICIOUS TRANSACTION REPORTS

MLRO will maintain the following records on suspicious reports:

1. Internal Disclosure Forms received by the MLRO;
2. Internal suspicious transaction reports and suspicious transactions reports made to the FIU;
3. Where no suspicious report that has been made to the FIU, record of information or material that was considered and the evaluation report mentioning the reason for the decision will be retained.

These records should be retained 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 to which they relate.

Structure and Procedure

Reporting Structure

STAFF MEMBER → MLRO / DEPUTY MLRO → FIU

i. It is the duty of each staff irrespective of his/her status in the Company to report to the MLRO/ Deputy MLRO, any transaction of a suspicious nature.
ii. The MLRO/ Deputy MLRO shall investigate the internal STR and decide if the same is founded.
iii. The STR is then reported to the FIU via the GoAML Portal; along with the justification for the filing of the internal STR.

The Contact details of the FIU are as follows:

The Director
Financial Intelligence Unit
7th Floor, Ebène Heights
34, Ebène Cybercity
Ebène
Tel: (230) 454 1423
Fax: (230) 466 2431
Email: fiu@fiumauritius.org
GoAML Portal: https://www.mrugoaml.fiumauritius.org/goAMLWeb_PRD/Account/LogOn

5.9 REVIEW OF THE AML/CFT POLICIES, PROCEDURES AND PROCESSES AND INDEPENDENT AUDIT

The contents of this Manual shall be reviewed by the Compliance Officer / MLRO / DMLRO as and when required and the following procedures shall be adhered to in the event of amendments to the Manual:

- Submission of the amended Manual to the Board for approval.
- The approved Manual shall be communicated to all the Officers and staff administering the Company as soon as possible.
- Officers and staff administering the Company (including officers / staff of the MC assigned to administer the Company) shall read and acknowledge having read the Manual. (Appendix 12)

5.10 INDEPENDENT AUDIT FUNCTION

As per Regulation 22(1)(d) of the FIAML Regulations 2018 and Chapter 13 of the FSC Handbook, the Company is required to have in place an audit function to review and verify compliance with and effectiveness of the measures taken in accordance with the FIAMLA and FIAML Regulations 2018.
The independent audit function shall be responsible for:

a. The evaluation of the AML/CFT programme of the Company and ascertaining the adequacy of the established policies, procedures, systems, and controls in identifying ML/TF risks, addressing the identified risks, and complying with laws, regulations, and guidelines;
b. The effectiveness of the Company's employees and officers in implementing the company's policies, procedures, and controls;
c. The effectiveness of the compliance oversight and quality control including parameters and criteria for transaction alerts; and
d. The effectiveness of the Company's training of relevant employees and officers.

The frequency of the audit should be commensurate with the ML/TF risks presented and the size and complexity of the Company. An independent audit exercise shall be conducted at least once annually unless other material changes to the Company or legislative and regulatory obligations occur.

The findings of the independent audit report, highlighting recommendations and deficiencies, should be reported to senior management and to the board of directors. It is the responsibility of the board of directors of the financial institutions to take appropriate corrective actions to remediate any issues identified in the independent audit report within the specified timelines.

All independent audit documentation, including, inter alia, work plan, audit scope, transaction testing, should also be properly documented and shall be made available to the FSC upon request.

5.11 PENALTIES UNDER THE APPLICABLE LAWS RELATED TO AML/CFT

Failing to comply with applicable AML/CFT related laws could result in significant criminal liability. For instance, any person who commits a money laundering offence under the FIAMLA may be liable to a fine of up to 10 million rupees and to penal servitude for a maximum term of 20 years. Failure to comply with the CDD or reporting requirements under the FIAMLA could result in criminal liability of a fine of up to 5 million rupees and to imprisonment for a maximum term of 10 years. Contravention of the FIAML Regulations 2018 is also sanctioned through the imposition of a fine up to 1 million rupees and to imprisonment for a term of up to 5 years.

5.12 CERTIFICATION

5.12.1 Where the verification of identity documentation is not in an original form, the documentation must be appropriately certified as true copies of the original documentation.

5.12.2 Where an employee, director or officer of the Company meets the proposed client or the principals of a corporate client face-to-face and has access to original verification of identity documentation, he/she may take copies of the verification of identity documentation and certify them personally as true copies of the original documentation.

5.12.3 In other cases, copies of the verification of identity documentation should be certified by a suitable person such as a lawyer, notary, actuary, an accountant, or any other person holding

a recognized professional qualification, director or secretary of a regulated financial institution in Mauritius or in an equivalent jurisdiction, a member of the judiciary or a senior civil servant.

5.12.4 The certifier should sign the copy document and clearly indicate his name, address and position or capacity on it together with contact details to aid tracing of the certifier.

5.12.5 The Company is responsible to ensure that the certification is appropriate. Caution must be taken when considering certified copy documents originating from a country perceived to represent a high risk or non-equivalent jurisdictions.

5.12.6 In all cases, the Company must also ensure that the representative of the client's signature on the identification document matches the signature on the application form, mandate, or other document.

5.12.7 Where digital tool are being used, the authenticity of the documents is verified by the platform which uses high-end technology to determine the accuracy of the documents.

5.13 TRANSLATION

5.13.1 Where any of the documents is in a language other than English or French, it should be translated into either of these languages by any one of the followings:

a. Qualified translator;
b. An employee of the Company who is a native speaker of the said language and fluent in English or French;
c. Translation Software(s).

5.13.2 The translator should sign the document and clearly indicate his name, position, company, email address and date of the translation to aid tracing of the translator.

In order to ascertain the appropriateness of the certifier and the suitability of the translator(s), independent checks and verification of documents shall be conducted and sought respectively.

SECTION 6: CLIENT POLICIES AND PROCEDURES

6.1 GENERAL CLIENT POLICY

It is the general policy of the Company to have a staff of appropriate calibre as the prime contact to any client. Client meetings are summarised in a Minutes of Meeting which is held on record in the corresponding client file.

Prior to incorporation/set-up of the entity(ies), the Company shall ensure that the Client understands the nature of the risks involved in the different types of investment/products proposed. Please refer to the Risk Disclosure Policy.

6.2 CLIENT ON-BOARDING POLICY

6.2.1 LIVE ONBOARDING OF CLIENTS

The Client Onboarding refers to the process of getting new clients acquainted with the products and services which we offer. It defines how the Company establish first contact and relationship with the clients and they can derive the most value from the Company. It involves introducing clients to our business which includes guidance, support, and step-by-step tutorials.

The onboarding of clients is as follows:

- Client will access the website of the Company in order to open of an account on its platform;
- Client is requested to complete the application form and submit all Customer Due Diligence ("CDD") documents;
- The Onboarding Team / Backoffice Team will ensure that all sections of Application form are completed in full; if the information is missing, the Application form will be returned to the client for completion;
- After receiving the CDD documents, the Onboarding Team / Backoffice Team of the Company will carry out identification, verification, and screening procedures as per the policy of the Company;

Where the Client refuses to provide the information or such information as may be required, when requested, or appears to have intentionally provided misleading information, the Company will not proceed with opening an account for the client.

Amongst others, factors that must be considered prior to entering into any relationship with the client include the client's background, his/her/its country of origin, his/her public or high-profile position, his/her business activities, delivery channels, client's risk appetite and other risk factors. More extensive due diligence must be conducted for higher risk clients.

No client will be accepted by the Company unless his/her background and source of funds/wealth is fully understood or if the client originates from one of the following sources:

- The client is an existing well-known client of the Company of good standing who wishes to open an additional client account with the Company
- The client is a well-known local or international or regulated company of good repute
- The client is referred by a Management Company, a law firm, a bank, or any other professionals that are rigorously regulated in the business activity in which they are engaged
- The client is referred by a director or shareholder or member of the Management of the Company
- The client is referred by a trusted individual or entity with which the Company has established a proven working relationship.

Please also refer Section 5.0 on Client Identification and Verification Procedures.

6.2.2 POST ONBOARDING OF CLIENTS

Once the Onboarding Team / Backoffice Team complete the verification of the CDD documents and screening on the clients, the Compliance Analyst of the Management Company shall conduct a second verification of documents and screening on the clients.

- The Proof of Identities and Proof of Addresses are verified together with the application forms of the clients. In case, the application form is not available, the CRM is used for more details.
- In case of PEP or adverse matches, EDD documents shall be requested from the Company.
- The Compliance Analyst, shall, then risk rate the clients depending on the information gathered.
- Real time Transaction Monitoring is conducted by the Operation Team.
- Transaction Reports are provided on a daily basis (within 24hrs). The Management Company, therefore, conducts its transaction monitoring.
- Additional and/or Updated documents are requested as and when applicable.
- In cases where it is difficult to ascertain the source and flow of funds, the information on the application form is incomplete or the amount of deposits made cannot be tallied with the information disclosed on the application form, the Management Company will then request for any of the following:

a) Signed Declaration of Source of Funds and Wealth;
b) Any relevant supporting documents
c) A Professional Reference/ CV might be requested to ascertain same; optional.
d) The Company will also ensure to conduct Internet Search and Sanction checks

The Company ensures;

a. collecting certain identification information from each customer who opens an account;
b. utilizing risk-based measures to verify the identity of each customer who opens an account; and
c. recording customer identification information and the verification methods and results.

The Company shall take reasonable measures at the time of establishing a business relationship to determine whether the applicant for business is acting on behalf of a third party. In the affirmative, it shall then keep a record setting out -

(i) the identity of the third party (and any associated persons as required);
(ii) the proofs of identity required under Regulation 3 of the FIAML Regulations 2018; and

6.2.3 MIGRATION PROCESS

- The Company will inform the Management Company in case of any migration and will share the list of migrated clients.

- The Management Company shall guide the Company that prior to onboarding of the ''migrated clients'', they will need to ensure that their documents are up to date, duly certified and translated.

- It is imperative for the clients to know that their accounts are being migrated to another entity and hence they will be requested to provide updated documents, where applicable. (If possible an authorization letter and/or email can be requested/sent and/or any other tick box online option/pop ups when they login – the client accept to migrate his account).

- As Mauritius does not transact with Democratic People's Republic of Korea, Iran and Myanmar, these clients will not be migrated. The ID can either opt to migrate them to another entity or close their accounts - If their accounts are funded, their funds will be returned to them – As such an Account Closure Form and/or email can be implemented (same clause will be added, the client will only acknowledge that their accounts will be closed, and funds will be returned). Alternatively the client may be migrated to a group entity in another jurisdiction.

- In cases where it is difficult to ascertain the source and flow of funds, the information on the application form is incomplete or the amount of deposits made cannot be tallied with the information disclosed on the application form, the Management Company will then request for any of the following:
    a) Signed Declaration of Source of Funds and Wealth;
    b) Any relevant supporting documents

- The Management Company shall ensure Screening, Internet Search, UNSC checks and Risk Assessment on the migrated clients. The Client Risk Assessment of the clients shall be reviewed depending on their risk rating.

- The MC shall, then, notify the FSC about the migration.

6.2.3.1 THE CLIENT ONBOARDING RELIES ON THE FOLLOWING FUNDAMENTAL PRINCIPLES:

a. Each document must be identified as true copies of the original documents.
b. Documents can be certified by one of the following;
    1. Where an employee, director or officer of the Company meets the proposed client or the principals of a corporate client face-to-face and has access to original verification of identity documentation, he/she may take copies of the verification of identity documentation and certify them personally as true copies of the original documentation.
    2. Where there is no personal contact, obtain a copy certified as a true copy by an Attorney, a Barrister, a Notary, or a Chartered Accountant.
    3. The certifier should sign the copy document and clearly indicate his/her name, address and position or capacity on it together with contact details for identifying the certifier.

c. Application will not be accepted if the identification proves to be incomplete. For all accounts, if applicable for any person, entity or organisation opening a new account and whose name is indicated on the account;

    1. Name, incorporation number, legal status, date and country of incorporation or registration (for an entity other than an individual);

    2. Date and place of birth (for an individual)

    3. Occupation, public position held and where appropriate, the name of the employer (for an individual) or Anti-Money Laundering and Counter-Terrorism Financing Policy (for an entity other than an individual)

    4. A current address, which will be residential (for an individual) or registered office address and principal place of business (where different from the registered office, for an entity other than an individual)

    5. Passport number and country of issuance, identification card number and country of issuance of any other government issued document evidencing nationality or residence and bearing a photograph or other similar safeguard e.g. national identity cards, current valid passports, or current valid driving licenses; and

    6. The identity of underlying principles (including beneficial owners, controllers, directors or equivalent) with ultimate effective control over the capital or assets of an entity other than an individual in addition to evidence that any person who purports to act on behalf of the legal person is duly authorized and identify that person.

d. Where the underlying principals are not individuals, the Company shall investigate further to establish the identity of the natural persons ultimately owning or controlling the business. When opening an account for a foreign business or enterprise that does not have identification number, the Company will request alternative government approved documentation certifying the existence of the business or enterprise.

e. If potential customer refuses to provide the information described above or such information as the Company may require or appears to have intentionally provided misleading information, the Company shall not open a new account and, after considering the risks involved, will consider closing any open account(s) of an existing customer.

f. Risk profile of the Customer is determined based on those documents. If the risk is found to be higher than average, enhanced due diligence may be necessary before on boarding the customer and/or ongoing close monitoring of Customers transactions might be necessary or sufficient. The Company ensures to all reasonable and practicable that the sanction screening of each Customer as per section 5.7.

g. After the final assessment and before entering in a business relationship with the customer, the risk profiling sheet must be signed by the Compliance Officer, thus giving acceptance to proceed the on boarding of Customer.

h. All documents will be recorded for a minimum period of seven (7) years from the date of the on boarding of the Customers.

6.3 PRINCIPALS AND OFFICERS OF THE COMPANY

For any CDD measures which are being carried out on the Principals and Officers of the Company, for instance, the Directors, Shareholders, Ultimate Beneficial Owners, Head of Dealings, Assistant Head of Dealings, MRLO, Deputy MLRO and Bank Signatories and all the CDD documentation should be duly certified as true copy of the originals in line with the requirements of the FSC.

6.4 CLASSIFICATION OF CLIENTS

Clients are classified in 3 buckets:

1. Active
2. Inactive / Dormant
3. Closed

1. <u>Active Clients</u>

''Active Clients'' means any natural or legal person who have been registered with the Company and have transacted or traded within the last 6 months.

Standard Due Diligence is conducted on all clients as stipulated in *Step 2 – Identification and Verification*, and Updated CDD documents are requested as per Appendix 11 of the AML/CFT Compliance Manual.

2. <u>Inactive Clients</u>

The Inactive / Dormant Account status is defined by multiple criteria: (i) absence of open positions for 6 consecutive months, (ii) no trade activity in the last 6 consecutive months, (iii) no deposit, withdrawal, or internal transfer activity in the last 6 consecutive months. An internal transfer between the Accounts is not regarded as a deposit or a withdrawal.

Standard Due Diligence is conducted on all clients as stipulated in *Step 2 – Identification and Verification*. Whereby the client is classified as Inactive / Dormant due to inactivity as defined above, updated documents will **NOT** be requested.

Procedures for reactivation of Inactive accounts:

If a client wants to deposit or trade from/to his account, and his/her account was inactive due to dormancy, then the following procedure will be followed before allowing the client to deposit or trade:

- **i.** Updated Proof of Address (not later than 3 months) and Updated Proof of Identity (where applicable) will be required.
- **ii.** Any prior additional information requested (for e.g, information on application form, source of funds/wealth amongst others) should be provided.
- **iii.** Screenings (Worldcheck, Sanction Screenings & Internet Search) will be re-conducted.
- **iv.** Risk Assessment will be revisited and shall be updated as applicable.

3. Closed Accounts

''Closed Accounts'' means any account which have been registered with the Company but are deemed closed due the following circumstances but not limited to:

- **i.** Internal Policy* (outdated CDD documents, lack of Information, patterns of transactions amongst others)

  Prior to the closure of the account, the client will be notified and given a delay of 2 weeks to provide updated CDD or any further documentation. If the documents requested are not provided within the timeframe, the account will be closed.

  The Company may at its discretion proceed to freeze the account of the client if it considers that documents received are not adequate and the client fails to provide the documents within the deadlines advised by the Company. In this case the account of the client will be charged a handling fee of $5 per month or the balance of the account whichever lower until the client provides the Company with the missing information.

- **ii.** Inactive over a period of 24 months*

  Upon the Account reaching 24 months of inactivity, an automated message will be triggered and dispatched to the Client, notifying them about the forthcoming account

deduction in accordance with the Terms. Simultaneously, the sales team will be notified of these actions.

Once the Account balance reaches zero, it will be disabled. Three months after the deactivation, the Account will be closed from MT trading system and Client portal. The master Account, however, will remain untouched. If all trading Accounts are closed, the master Account status will be closed.

iii. Upon Client's Request

Further to the closure of account upon the request of the client, the account cannot be reactivated. The client will have to open a new account with the company.

The Company shall keep its own office records and those its Clients for a period of 7 years as required under the companies Act 2001 and the Financial Service Act 2007.

In the Event of Death

1. In the event of the Client's death, any person(s) purporting to be the Client's legal personal representative(s) must provide the Company with formal notice of the Client's death in a form acceptable to the Company, including but not limited to the provision of an original death certificate in physical form.

2. Upon the receipt and acceptance of the Client's death certificate, the Company will treat the Client's death as an Event of Default allowing the Company to exercise any of its rights including but not limited to closing any and all Open Positions within the Client's Account. The Agreement will continue to bind the Client's estate until terminated by the Client's legal personal representative or by the Company in accordance with these Terms.

3. A person shall not be proven to be the Client's legal personal representative until the Company receives a grant of representation for the Client's estate. Once the Company receives the grant of representation for the Client's estate, the Company will carry out the written instructions from the Client's legal personal representative(s). The Company will only accept instructions that aim to wind-down and/or close the Account. No registered asset may be sold until any re- registration process is completed and all fees, charges and expenses which may be owed by the Client to the Company are accounted for. Where the Company has not received any instructions after six (6) months following receipt of the Client's death certificate, the Company may (but shall not be obliged) re-register the Client's holdings into the name of its legal personal representative, re-materialize any electronic holdings and send such holdings in certificated form to the registered correspondence address for the Client's estate, subject to appropriate charges detailed from time to time in the Financial Terms.

4. If the Client's estate is too small to warrant a grant of representation, the Company may in its sole and absolute discretion, require any person(s) purporting to be the Client's legal personal representative(s) to obtain a grant of representation or request an appropriate indemnity.

5. Any applicable charges as detailed in the Financial Terms will continue to be charged until the Account is closed.

6. Notwithstanding anything in the Agreement, if the Agreement is not terminated within two (2) years after the date of the Client's death, the Company may take such action as it considers appropriate to close the Client's Account. The Client's estate or its legal personal representative(s) will be liable for all costs associated with the Company taking this action, or considering taking action, except to the extent that costs arise because of the Company's gross negligence, willful default or fraud.

SECTION 7: OPERATING POLICIES AND PROCEDURES

7.1. CLIENT OPERATIONAL PROCEDURES

It is the objective of the Company to provide clients with tailor made solutions with tangible benefits and returns in an environment of satisfaction and trust. The Company has put in place various client operational procedures to fulfil this objective. These operational procedures will also ensure that the Company monitors promptly its compliance programme in accordance with its policies and procedures.

7.2 SERVICES TO CLIENTS

- The Company shall ensure that customers are provided with accurate, timely and comprehensible information that would enable them to make informed decisions.

7.3 SEGREGATION OF CLIENTS' BANK AND COPRORATE ACCOUNTS

The Company shall ensure that, where it has control over the clients' assets (including clients' money), these are, at all times, properly segregated and identifiable.

The Company has put measures in place with respect to segregation of clients' funds. The Company has adopted the policy of not mixing its assets with those of its clients/customers. The Company shall ensure that the assets of a client (including cash at bank) are clearly identified and held separately from the assets of the Company and the assets of any other client.

7.4 REPORTING TO CLIENTS

As a business practice, the Investment Dealer issues ''Statement of Accounts'' to the traders/end clients on a daily/weekly/monthly basis depending on the volume of the transactions or upon request of the traders/end clients.

- The ''Statement of Accounts'' covers the following sections:
- First time deposit of the traders/end clients.

- Open or closed trades placed.
- Margin Calls.
- Other deposits made by the traders/end clients.
- Withdrawal(s) placed.
- Current account balance.
- Total profit and loss.

As a whole, the statement provides an overview of the trading account.

7.5 ADVANCES BY THE COMPANY

The Company shall not enter into the following transactions:

1) It shall not make any advance to his client by way of loan, to be applied to buy securities unless—
    a) before the advance is made, the client has executed a contract that sets out the terms on which the advance is made, and such contract complies with the FSC Rules; and

    b) the amount advanced does not exceed the percentage of the market value of the securities specified in FSC Rules made for the purposes of this paragraph.

2) Failure to comply with (1) above shall tantamount to an offence and shall, on conviction, be liable to a fine not exceeding 500,000 rupees.

3) Additionally, under section 54 of the SA 2005, any credit balances in the accounts of a client of the Company, not representing securities that are pledged, mortgaged, subject to a lien or other security interest or given to support a guarantee or similar arrangement, shall—

    a) be payable on demand;
    b) not be used or applied by the investment dealer without the express written authority of the client; and
    c) not form part of the assets of the investment dealer for the purposes of the law relating to insolvency.

4) Failure to comply with (3) above shall give rise to an offence and shall, on conviction, be liable to a fine not exceeding 500,000 rupees.

5) The Company shall be liable to pay its client interest, calculated in accordance with the market rate, on the credit balance in the securities accounts of the client maintained by it.

7.6 CONFLICT OF INTEREST

The Company endeavours to take such actions as may be necessary to mitigate the risk of any conflict of interest.

All conflicts of interest and potential conflicts of interest shall have to be disclosed to, reviewed, and resolved (if applicable) by the Board of the Company.

In case there are any conflicts between the interest of a client and the interests of the Company, the Company shall give priority to the client's interest.

The Company has adopted a Management of Interest Policy as per Appendix 15. The Company shall be also guided by its Compliance Manual, its constitution, and the laws of Mauritius.

A Register of Interests (Appendix 15) shall be maintained by the Company.

7.7 COMPLAINTS HANDLING PROCEDURE

A complaint is an instance when the Company is informed by any of its customer that the service provided has not met the required expectations or by a stakeholder of any relevant issue. Complaints may be in writing or verbal. All complaints must be promptly investigated as they may indicate that procedural or service deficiencies have arisen. A further important reason for taking prompt action to complaints is that there may be an indication of serious irregularities or fraud.

The following procedure must be followed for any complaints:

- Acknowledge receipt of the complaint within 5 working days from the date the complaint has been received.
- Submit the complaint with all relevant information to the Compliance Officer without delay.
- Upon receipt of the complaint from a member of staff, the Compliance Officer shall:
- Gather any additional information required and investigate taking into account all aspects of the complaint, both internal and external.
- Where the complaint is as a result of an error on the part of the Company, immediate corrective actions must be taken to avoid recurrence of such issues.
- Resolve the complaint and ensure resolution is fair.
- Issue a written reply to the complainant which shall include (i) details of the findings, (ii) an apology, if the situation warrants (iii) any proposed resolution.
- Ensure that the client is satisfied with the response given.
- Cause such complaint to be recorded in the complaint log which shall be maintained by the Compliance Officer.

The written reply shall be given to the complainant as soon as practicable but not later than one month as from the date the complaint has been received.

Complaints evidencing fraud or malpractice must be referred to the MLRO/DMLRO forthwith for investigations and subsequent reporting as may be required.

7.8 COMPLIANCE AND RISK COMMITTEE

AML/CTF is a standing item on the Compliance and Risk Committee agenda. Compliance and Risk Committee Meetings take place as and when required. The Company has established the Compliance

Committee to supervise the Company's overall current and future risk appetite, oversee the senior management's implementation of the risk appetite framework and reporting on the state of risk.

For more information, please refer to the 'TERMS OF REFERENCE OF THE COMPLIANCE AND RISK COMMITTEE'.

7.9 AUDIT COMMITTEE

The Audit Committee assists the Board in fulfilling its responsibility with respect to;

(i) Ensure the Company adopts, maintains and applies appropriate accounting and financial reporting processes and procedures;

(ii) Facilitating the independence of the external audit process and addressing issues arising from the audit process; and

(iii) Ensuring the Company maintains effective risk management and internal control systems.

For more information, please refer to the 'TERMS OF REFERENCE OF AUDIT COMMITTEE'.

CONCLUSIVE REMARKS

- The Company's senior management is dedicated to overseeing the AML/CTF program and have ultimate responsibility for ensure compliance. Responsibility for ensuring policies and procedures is carried out in a manner to comply with AML/CTF laws and regulations is delegated to the Company's Compliance Officer, Money Laundering Reporting Officer, and Deputy Money Laundering Reporting Officer.

- This Manual has been adopted by the Board. Any amendment to this Manual is subject to Board oversight and approval (i.e. the Board must formally adopt any amendment to the Manual).

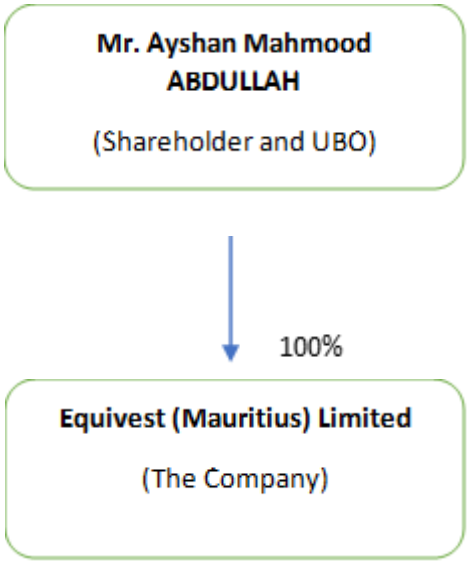
- At the start of their employment, every employee will be given a copy of this Manual and must sign the ''Acknowledgement Form'' (Appendix 12) to confirm that they have read and understood the provisions of this Manual. The signed form is then handed over to the MLRO for the file records. They will also need to undergo AML/CFT induction training for at least the duration of their probation period. It is the Firm's policy that they can only be confirmed to their positions once they have satisfactorily understood and completed their AML/CFT induction training.

- Each employee understands that a breach of any of the provisions of the Manual may result in criminal prosecution, regulatory sanction, and disciplinary action by the Firm, as may be the case.

LIST OF APPENDICES	
APPENDIX 1	The Company's Structure Chart
APPENDIX 2	Duties and Responsibilities of the MLRO and DMLRO
APPENDIX 3	Duties and Responsibilities of the Compliance officer
APPENDIX 4	Duties and Responsibilities of the Investment Dealer Team
APPENDIX 5	Risk Assessment Policy
APPENDIX 6A	Risk Assessment - Business Risk Assessment Questionnaire
APPENDIX 6B	Risk Assessment – Customer Risk Assessment Questionnaire
APPENDIX 7	PEP Declaration Form & PEP Register
APPENDIX 8	Training Log
Appendix 9	Internal STR Log
APPENDIX 10	Adverse Media / Compliance Reports
APPENDIX 11	Updated CDD Documents
Appendix 12	Acknowledgement Form
APPENDIX 13	Source of Fund Declaration Form
APPENDIX 14	List of Rejected Clients
APPENDIX 15	Management of Interest Policy Register of Interest
APPENDIX 16	Risk Assessment - Third Party Risk Assessment Questionnaire
APPENDIX 17	Transaction Monitoring Template

Appendix 1: The Company's Structure Chart

Structure Chart
Equivest (Mauritius) Limited



Appendix 2: Duties and Responsibilities of the MLRO and DMLRO

Adequate procedures should be implemented by Licensees to ensure that their MLRO has timely access to customer identification data and other CDD information, transaction records, and other relevant information in order to properly evaluate internal suspicious transaction reports.

MLROs must be autonomous in their decisions as to whether a suspicious transaction report should be made to the FIU.

MLROs may consult with colleagues as part of the evaluation process. However, the MLRO must be free to make his or her decision and without undue influence, pressure or fear of repercussions in the event that senior colleagues disagree with his/her decision. Where a MLRO validates an internal report about a transaction that has aroused suspicion, he/she has a legal obligation to make a report to the FIU.

The MLRO and Deputy MLRO in the absence of the MLRO:

- is the main point of contact with the Financial Intelligence Unit ("FIU") in the handling of disclosures;
- has unrestricted access to the CDD information of the Company's customers, including the beneficial owners thereof;
- has sufficient resources to perform his or her duties;
- is available on a day-to-day basis;
- reports directly to, and may have regular contact with the Board; and
- is fully aware of both his personal obligations and those of the Investment Dealer under FIAMLA and FIAML Regulations 2018, the FSC Handbook and this Compliance Procedures Manual.

Additionally, the MLRO is responsible for developing, maintaining and implementing plans in relation to money laundering and terrorist financing deterrence procedures, which shall comprise of the following:

- Designing appropriate system for the management of money laundering and terrorist financing risks;
- Providing advice and organizing training sessions on anti-money laundering and prevention of terrorist financing;
- Acting as the central point of contact for receipt of Money Laundering Suspicious Reports made by staff and subsequent validation, reporting and liaison with the FIU;
- Keeping records on money laundering and terrorist financing suspicion and advise the Company on necessary course of action concerning client relationship when filing a suspicious transaction report;

- Monitoring the risk rating of each client;
- Where necessary, updating the Manual with regards to money laundering and terrorist financing matters for consideration by the Board of Directors;
- Reporting of all money-laundering and terrorist financing issues to the Board on a annual basis, or at shorter interval, if required;
- Undertaking a review of all internal disclosures in the light of all available relevant information and determining whether or not such internal disclosures have substance and require an external disclosure to be made to the FIU;
- Maintaining all related records;
- Providing guidance on how to avoid tipping off the customer if any disclosure is made; and
- Liaising with the FIU, and if required with the FSC, and participating in any other third-party enquiries in relation to money laundering or terrorist financing prevention, detection, investigation or compliance.

Appendix 3: Duties and Responsibilities of the Compliance Officer

In accordance with Regulations 22 (1) (a) of FIAML Regulations 2018, the financial institution shall designate a compliance officer at senior management level and approved as officer under Section 24 of the FSA.

The Compliance Officer ('CO') is responsible for the implementation and ongoing compliance of the financial institution with internal programmes, controls and procedures with the requirements of the FIAMLA and FIAML Regulations 2018.

Senior management is defined under the FIAML Regulations 2018 as an officer or employee with sufficient knowledge of the institution's money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure, and need not, in all cases, be a member of the board of directors.

In accordance with Regulations 22(3) of the FIAML Regulations 2018, the functions of the Compliance Officer include:

- Ensuring continued compliance with the requirements of the FIAMLA and FIAML Regulations 2018 subject to the ongoing oversight of the Board and Senior Management;
- Undertaking day-to-day oversight of the programme for combatting money laundering and terrorism financing;
- Regular reporting, including reporting of non-compliance, to the Board and Senior Management on an annual basis or at shorter intervals whenever required.
- Contributing to designing, implementing and maintaining internal compliance manuals, policies, procedures and systems for combatting money laundering and terrorism financing.

The Compliance Officer also ensures that:

- The Investment Dealer has an adequate system to comply with relevant laws, Guidelines, etc.;
- An appropriate system exists to monitor operational performances and make recommendations to rectify any deficiencies;
- He / she acts as the principal point of contact with the regulators.

The Compliance Officer is responsible for developing, maintaining and implementing plans in relation to compliance, which shall comprise of the following:

- Identifying key controls and inclusion in the Manual
- Designing checklists for monitoring compliance
- Conducting compliance checks
- Making appropriate recommendations where improvements are necessary
- Reporting findings to the Board, as may be required
- Organizing training sessions on compliance
- Updating the Board on new laws and regulations
- Monitoring the risk rating of each client
- Updating the manual for consideration and approval by the Board of Directors

The Compliance Officer must carry out compliance reviews to ensure that procedures and controls set out in the Manual are completed at all times. This should help ensure that the Investment Dealer operates within the parameters of the guidelines, codes and other regulations set out by the regulators.

While it is not anticipated that the Compliance Officer will personally conduct all monitoring and testing, the expectation is that he / she will have oversight of any monitoring and testing being conducted by the Company.

The circumstances of the Company may be such that, due to the small number of employees, the CO holds additional functions or is responsible for other aspects of the Company's operations. Where this is the case, the Company must ensure that any conflicts of interest between the responsibilities of the CO role and those of any other functions are identified, documented and appropriately managed.

The CO however should be independent of the core operating activities of the Company and should not be engaged in soliciting business.

For the avoidance of doubt, the same individual can be appointed to the positions of Money Laundering Reporting Officer ("MLRO") and CO, provided the financial institution considers this appropriate with regard to the respective demands of the two roles and whether the individual has sufficient time and resources to fulfil both roles effectively.

The Compliance Officer must report to the Board of Directors of his / her findings arising from the compliance reviews.

When a breach or potential breach is identified, the Compliance Officer shall forthwith notify the Board for needful action.

Appendix 4: Duties and Responsibilities of the Investment Dealer Team

The Company has appointed a Dealing Team – Head of Dealing and Assistant Head of Dealing – whereby the dealers facilitate trades on behalf of their customers and may act as the principal or the agent.

The Dealing Team will be responsible for the following but not limited to;

- Make important policy, planning, and strategy decisions.
- Develop, implement, and review operational policies and procedures.
- Oversee budgeting, reporting, planning, and auditing.
- Supervise traders and other personnel while ensuring regulatory and internal compliance.
- Supervise the Treasury Department.
- Monitor and handle client risk management during the intra-day trading session.
- Set up a trading system compatible with Reuters that triggers buy and sell signals on a daily basis.
- Liaise with banks to monitor the liquidity and manage the settlement among clients, the company, and the stock market.
- To study and analyse the condition of the market and conduct detailed research on the financial, social, and economic data and information.
- To recommend ideas and suggestions in order to improve the present algorithms or help in the creation of new ones.
- To design potential strategies related to trading and determine a course of action that needs to be taken.
- To evaluate the risk involved and make appropriate decisions and prepare the relevant reports.
- To constantly monitor and review the transactions to verify the accuracy and ensure that they are in conformance with the rules and regulations.

Appendix 5: Risk Assessment Policy

1. What is a Risk Based Approach?

A Risk Based Approach is a mechanism which will be used by Credentia International Management Limited ('CIML' or 'the Company') to assess risks that potential, new and existing clients/partners/stakeholders may pose to the Company directly or indirectly. It is of utmost importance for CIML to make an initial assessment of the risks to which it may be exposed through the business relationship or proposed business relationship.

There are many factors which the Company has to take into consideration to evaluate potential risks a client/partner/stakeholder may pose. A non-exhaustive list of these elements is provided below:

- The Nature and type of customer/partner/stakeholder
- The Commercial rationale for the relationship
- The geographical location of the customer/partner/stakeholder residence
- The geographical location of the customer/partner/stakeholder business interests and / or assets (as may be applicable)
- The nature and value of the assets /funds concerned in the relationship
- The customer/partner source of funds and wealth, as appropriate
- The role of any introducer and whether it is regulated or not

2. How is the Risk Based Approach implemented?

CIML Risk Based Approach is implemented through the conduct of the Client Risk Assessment ("CRA") and the Business Risk Assessment ("BRA"). A Risk Profiling Questionnaire has been designed for each of the aforementioned Assessment, and same are annexed to this document, herein marked as '**Risk Profiling Questionnaire**' – **Annexure 1** and '**Business Risk Assessment**' – **Annexure 2**

The Client Risk Assessment – Risk Profiling Questionnaire:
In practice, the file Administrator or the Compliance Analyst, dedicated to the Company, will have to fill in a Risk Profiling Questionnaire, which comprises of specific questions to assess potential risks. The person then inserts the corresponding percentage he/she judges represents the level of risks attributable per criteria.

The total percentage attributed is then computed and the result is used to determine the level of risk of the client / business relationship.

The assessment is then counter-verified and validated by the Money Laundering Reporting Officer / Compliance Officer in line with the four eyes principle.

The Business Risk Assessment:
The Company should at all times avoid the "tick box" approach, and always has to determine the risks itself, based on its respective circumstances.

In so doing, this document or questionnaire is generally filled in by the Compliance Officer / Money Laundering Reporting Officer, adopting the same principle as mentioned above. The Company will take appropriate steps to mitigate any risks which have been identified and this will involve determining the necessary controls or procedures that need to be in place in relation to a particular part of the business in order to reduce the risk identified.

The document is then tabled to the Board of Directors of the Company for discussions and consideration. Ultimately, the BRA is validated and counter-signed by a member of the Board of Directors.
The full implementation of the above processes is detailed in Section 4. (The Procedures) below.

3. Why adopt a Risk Profiling System?

A proper Risk Profiling system helps the Company to assess clients, service providers, business relationships and/or activities and allocate effectively its resources and hence, reduces costs related directly to the internal Compliance Framework.

With an adequate Risk Profiling system implemented, CIML will be able to:

1. Assess and identify risks relating to clients/prospective clients, service providers, business relationships/activities, high risks situations.
2. Categorize and attribute the client/prospective client, business relationship/activities, situation, a risk level (Low, Medium, and High).
3. Allocate resources effectively to manage and mitigate risks.

4. The Procedures

The Client Risk Assessment – Risk Profiling Questionnaire:
PHASE 1
The file Administrator or the Compliance Analyst dedicated to the specific Client file will fill in the Risk Profiling Questionnaire (the 'Questionnaire') and according to his/her knowledge of the client/partner/stakeholder/service provider, compute the result and determine the risks attributable to the client/partner/stakeholder/service provider, his activity and / or the business relationship.
The file Administrator or Compliance Analyst then signs the Questionnaire.

PHASE 2
The Compliance Officer / MLRO will then review the Risk Profiling Questionnaire, amend if necessary and sign same to evidence the review.

PHASE 3
The Risk Rating (as provided in the below table under Section 6) is established and the Client file shall be reviewed in accordance with the Risk Rating attributed.

PHASE 4

In the event where a client file is categorized as High Risk, Enhanced Due Diligence (EDD) measures should be applied in accordance with the provisions of the Financial Intelligence and Anti-Money Laundering Regulations 2018 and the FSC Handbook 2020, as updated in March 2021.

In case where a Politically Exposed Person (PEP) has been identified during the business relationship, the Client file should be categorized as High Risk automatically, EDD measures applied, and approval of Senior Management / Board of Directors sought to continue / start / cease the business relationship.

The Business Risk Assessment:

PHASE 1

The Business Risk Assessment Questionnaire (the 'Questionnaire') should contain the followings:

- A Company Profile
- Align information with respect the approved Business Plan
- Overview of:
    - The main products and services
    - The main category of customers
    - Delivery channels
    - Geographical locations / spread of customers
    - Technological developments
    - Third party reliance for CDD Measures
- Assessment period under review

PHASE 2

The Compliance Officer / MLRO of the Company will fill in the Business Risk Assessment Questionnaire containing the above criteria and according to his knowledge of the activities of the Company, compute the result and determine the risks attributable to the Company.

PHASE 3

The Compliance Officer / MLRO then signs the Questionnaire.

PHASE 4

The document is then tabled to the Board of Directors of the Company for reviews, discussions and consideration. Any changes or input will then be considered.

PHASE 5

Eventually, as soon as the Board approval is obtained, the BRA is validated and counter-signed by a member of the Board of Directors.

The ultimate responsibility for the Business Risk Assessment lies with the Board of Directors of the Company.

5. Change in Risk Rating

The risk assessment may change as and when there may be any trigger event. It may happen that, upon the occurrence of a specific event, or situation, it becomes obvious that the Risk Rating needs to be amended, that is, either increased or decreased. This change in Risk Rating should be re-approved by the Compliance Officer / MLRO, upon recommendation of the Compliance Analyst or file Administrator.

The purpose of these reviews is to identify any significant changes to the corporate structure, management and activities of the client. Unless the MLRO resolves otherwise, it is not always necessary to obtain all the information required for account opening or to re-verify all identification information. These reviews are validated by the Compliance Officer / MLRO. In addition to reviewing changes to the client's structure, management and profile an overall review of the client's activity over the period is normally conducted. This will allow the Company to assess if there have been changes in the client's activity which could be considered unusual given the information held about the client. Notwithstanding these timescales, should any employee become aware of a change in the circumstances of a client, for example change of ownership structure or move into a new business area, this information should be recorded on the client file immediately. If this information could affect the risk assessment of the client, then the Compliance Officer / MLRO should be informed. The Compliance Officer / MLRO will then decide if there is the need to re-evaluate the client's risk assessment.

Instances where there may be a trigger event are as follows, though the below is non-exhaustive:

- Change in Jurisdiction
- Change in Nationality
- Change in Products and Services
- Change in Nature and Value of the Assets

6. Level of Risk

The Client Risk Assessment – Risk Profiling Questionnaire:

Risks will be classified into three categories as described below, and this will determine the frequency of review of the client files.

Risk Level:	**Frequency of Review:**
Low	Every 3 years
Medium	Every 2 years
High	yearly

The Business Risk Assessment:

Risks will be classified into three categories as described below, and the frequency of review will be Annually.

Risk Category:	**Risk Rating:**	**Risk Guidance:**
Low	0 - 35	0 – 5 5 = Not Compliant (High Risk)
Medium	36 - 75	

High	76 – 135	3 = Less Compliant (Medium Risk) 1 = Nearly Compliant (Low Risk) 0 = Fully Compliant (No Risk)

7. Risk Rating and Guidance

The Client Risk Assessment – Risk Profiling Questionnaire:

After computing the risks in the Risk Profiling Questionnaire, the below table should be used to categorize the risk level of the client file / structure.

Risk level	**Risk Rating**
Low	0 - 59
Medium	60 - 129
High	130 - 200

The following should be used as guidance when applying a risk-based approach to the assessment of money laundering risk posed by each Client / Service Provider. Consideration of the overall information held or gathered through the application process may alter the risk profile.

Low and Medium Risk:

- Regulated credit or financial institutions located in equivalent jurisdictions and FATF Member Countries;
- A publicly traded company or investment fund listed on an equivalent exchange;
- A regulated investment fund located and regulated by a body having equivalent regulatory and supervisory responsibilities as the FSC.
- Where, for instance, Customer Due Diligence measures is not yet completed.

High Risk:

- Relationships where a PEP or their connected person has been identified as having a significant involvement (This definition of PEP would include heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of publicly owned enterprises and important political party officials);
- Complex business ownership structures, such as offshore special purpose vehicles, that make it easier to conceal underlying beneficial owners, especially where there is no legitimate commercial rationale;
- Relationships involving clients that reside in or nationals of Non-Cooperative Countries and Territories (“NCCTs”);
- Accounts that involve regular payments to or from unrelated third parties;
- Names that have been previously linked with financial crime (these can be found in the UN Sanctions List: https://www.un.org/securitycouncil/content/un-sc-consolidated-list);
- Clients based in or conducting business in or through high-risk jurisdictions with known level of corruption and organized crime, or drug production and distribution;
- Clients engaged in higher risk business activities (e.g. electronic gambling/gaming via the internet);
- Companies issuing bearer shares, especially if incorporated in higher risk jurisdictions;
- Clients that have been subject to a Suspicious Transaction Report.

The Business Risk Assessment:

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

(i) the nature, scale and complexity of the Company's activities;
(ii) the products and services provided by the Company;
(iii) the persons to whom and the manner in which the products and services are provided;
(iv) the nature, scale, complexity and location of the Clients' activities;
(v) reliance on third parties for elements of the customer due diligence process; and
(vi) technological developments.

As per Section 17(2) (b) of the FIAMLA, the Company will have to take into account the findings of the National Risk Assessment ('NRA') and any guidance issued in its Business Risk Assessment.

8. Useful Publicly Available Sources

- The FIAMLA 2002

http://www.fiumauritius.org/English/AML%20CFT%20Framework/Documents/2020/FIAMLA%20Updated%20August%202020.pdf

- The FIAML Regulations 2018

http://www.fiumauritius.org/English/AML%20CFT%20Framework/Documents/FIAMLA-2018.pdf

- The FSC Handbook 2020

https://www.fscmauritius.org/media/99188/aml-cft-handbook.pdf

- The National Risk Assessment Report

https://financialservices.govmu.org/Documents/NRA%20Report/Public%20Report%202019-compressed.pdf

- Findings of the National Risk Assessment on Money Laundering and Terrorist Financing of Mauritius

http://www.fiumauritius.org/English/Seminars/Documents/NRAWorkshopPresentationsWebsite14102020.pdf

Appendix 6A: Business Risk Assessment Questionnaire

BUSINESS RISK ASSESSMENT – INVESTMENT DEALER'S NAME ('XXX')

Date of Review: XXX	**Date of Next Review: XXX**
RISK RATING: XXX/135	**Overall Risk Level:** ▪ **Low Risk** ☐ ▪ **Medium Risk** ☐ ▪ **High Risk** ☐
Period Covered of BRA:	**XXX TO XXXX**

	Risk Assessment Criteria	Inherent Risk Rating Guide	Likelihood Risk Rating	Inherent Risk Level	Risk Mitigating Measures
I.	**RISKS RELATED TO THE NATURE, SCALE AND COMPLEXITY OF OUR ACTIVITIES**	**1-5 LOW 6-15 MEDIUM 16-25 HIGH**	**RATING XX/25**	**LOW /MEDIUM /HIGH**	**See Below**
(a)	To what extent can our services be abused for ML/TF without our knowledge?	**1 – 5**			
(b)	Risks (threats and vulnerabilities) posed by ML/TF within those areas for which senior management has responsibility	**1 – 5**			
(c)	Any organisational factors that may increase exposure to the risk of ML/TF (e.g. investment/assets under management volumes and outsourcing aspects of regulated activities or compliance functions)?	**1 – 5**			
(d)	Nature, scale and complexity of our business including the diversity of its operations, the volume and size of its transactions, and the degree of risk associated with each area of its operation	**1 – 5**			
(e)	Any particular threats from high-risk jurisdictions, any particular vulnerabilities within the organisation in those jurisdictions?	**1 – 5**			
	Comments on Mitigating Factors Applied to the Residual Risk:				

2.	RISKS RELATED TO PRODUCTS AND SERVICES WE OFFER	1-5 LOW 6-15 MEDIUM 16-25 HIGH	RATING XX/25	LOW /MEDIUM /HIGH M	RISK MITIGATING MEASURES
(a)	Vulnerabilities of the services or products offered and how they could be abused for ML/TF	1 - 5			
(b)	Are payments to any unknown or un-associated third parties are allowed which would pose ML/TF risks?	0 - 5			
(c)	Are the products/services of particular or unusual complexity or using new technologies which we do not master?	1 – 5			
(d)	Proportion of business relationship conducted on a non-face-to-face basis	1 – 5			
(e)	Any reliance on introducers of business or other intermediaries and the nature of their relationship with us	1 – 5			
	Comments on Mitigating Factors Applied to the Residual Risk:				
3.	**PERSONS TO WHOM AND THE MANNER IN WHICH THE PRODUCTS AND SERVICES ARE PROVIDED**	**1-3 LOW 4-9 MEDIUM 10-15 HIGH**	**RATING XX/15**	**LOW /MEDIUM /HIGH**	**RISK MITIGATING MEASURES**
(a)	Threats posed by the types of customers: ▪ PEPs ▪ High Net Worth Individuals ▪ Those from or Operating in a Higher Risk Jurisdiction ▪ Non Face-To-Face Business	1 - 5			
(b)	High values and volumes - can unlimited third-party funds be freely received and/or can those funds be regularly paid to third parties without CDD on the third parties being obtained?	1 - 5			
(c)	Speed with which products and services can be delivered or transactions undertaken without proper verifications/checks	1 – 5			
	Comments on Mitigating Factors Applied to the Residual Risk:				
4.	**NATURE, SCALE, COMPLEXITY AND LOCATION OF THE CUSTOMER'S ACTIVITIES**	**1-5 LOW 6-15 MEDIUM 16-25 HIGH**	**RATING XX/25**	**LOW /MEDIUM /HIGH**	**RISK MITIGATING MEASURES**
(a)	Does customer base have any involvement in those businesses which are likely to be most vulnerable to	**Yes (5) No (0)**			

	corruption, such as oil, construction or arms sales				
(b)	Are customers from jurisdictions/territories known for: ▪ High level of predicate offences to ML, corruption, organised crime, tax crime and serious fraud? ▪ High vulnerabilities to corruption with inadequate frameworks to prevent and detect ML/TF? ▪ Providing funding or support for terrorist activities or that groups committing terrorist offences are known to be operating in the country or territory? ▪ Subject to financial sanctions, embargoes or measures that are related to terrorism, financing of terrorism or proliferation issued by, for example, the UN or the EU? ▪ Low capacity of its investigative judicial system effectively to investigate and prosecute these offences?	**Yes (5)** **No (0)**			
(c)	Complexity of customer and beneficial ownership structures	**1 – 5**			
(d)	Complexity of legal persons and legal arrangements	**1 – 5**			
(e)	Number of customers and beneficial owners which are charities or non-profit organisations (“NPOs”) and their associated countries or geographic areas	**1 – 5**			
	Comments on Mitigating Factors Applied to the Residual Risk:				
5.	**RELIANCE ON THIRD PARTIES FOR ELEMENTS OF THE CUSTOMER DUE DILIGENCE PROCESS**	**1-3 LOW** **4-6 MEDIUM** **7-10 HIGH**	**RATING XX/10**	**LOW /MEDIUM /HIGH**	**RISK MITIGATING MEASURES**
(a)	Any reliance on third parties for CDD? If yes, any reputational issues or any issues relating to the quality of the relationship(s) with such third party(ies) and previous experiences?	**1 – 5**			

	If yes, the extent and type of any reliance placed or to be placed on third parties. If yes, the extent of the information being provided by the third party and who has actually met the customer face-to-face (chains of information). If yes, any jurisdictional issues in connection with reliance placed on third parties. If yes, the results of any testing undertaken on the third party's procedures and the responses to any previous requests for documentation. If yes, the extent of any outsourcing undertaken.				
(b)	The quality of the **provider for any outsourced functions** including any reputational issues, previous experiences with the provider, results of any audits, assessments, or inspections where the material generated as a result of outsourcing has been reviewed.	**1 – 5**			
	Comments on Mitigating Factors Applied to the Residual Risk:				
6.	**TECHNOLOGICAL DEVELOPMENTS**	**0-5 LOW 6-15 MEDIUM 16-25 HIGH**	**RATING XX/25**	**LOW /MEDIUM /HIGH**	**RISK MITIGATING MEASURES**
(a)	Any digital information storage including cloud computing risks without mitigating factors? Any digital or electronic documentation storage risks without mitigating factors?	**0 – 5**			
(b)	Any electronic verification of documentation risks without mitigating factors?	**0 – 5**			
(c)	Any data and transaction screening systems risks without mitigating factors?	**0 – 5**			

(d)	Use of virtual or digital currencies?	**0 – 5**			
(e)	Operational/Reputational/Legal risks subsequent to technological developments?	**0 – 5**			
	Comments on Mitigating Factors Applied to the Residual Risk:				
7.	**Any additional relevant factor(s) to take into consideration?**	**(0-10)**	**XX/10**		
(a)	**Section 17 (2)(b) requires that the Risk Assessment shall take into account the outcome of any risk assessment carried out at a national level and any guidance issued.** **The following is applicable, amongst others:** • **National Risk Assessment** • **The FSC Handbook 2020, as amended in September 2022** **FATF Recommendations**	**Yes (0)** **No (5)**			
(b)	**Any other relevant factors taken into consideration**	**Yes (5)** **No (0)**			
	Comments on Mitigating Factors Applied to the Residual Risk: **This will be constantly reviewed should there be any material change at all affecting the risk score.**				
	TOTAL RATING	**(135)**	**XX/135**	**LOW**	

Overall Risk Level	Overall Risk Rating
Low	0 - 35
Medium	36 - 75
High*	76 – 135

**The organisation should identify and mitigate any arising risks, wherever applicable.*

OVERALL COMMENTS

Made on this XXX XXXX

Name:	**Name:**
Signature:	**Signature:**

Appendix 6B: Customer Risk Assessment Questionnaire

Name of Investor:		Date Review:
PART II - VI	**Overall Risk Rating:** **Overall Risk Level:** **Low Risk ('LR')** ☐ **Medium Risk ('MR')** ☐ **High Risk ('HR')** ☐	**Date of Next Review:**

I.	RISK ASSESSMENT - CLIENT ACCEPTANCE BASED ON PRELIMINARY CHECKS	GUIDE	SCORE	COMMENTS
(a)	Client is a Listed Party and/or its source of funds (premiums) are from a sanctioned jurisdiction or dealings or proposed dealings with a sanctioned jurisdiction	NO - 0 YES - 5		
(b)	Client's background not consistent with information about its former, current or planned business activity, business's turnover, etc.	NO - 0 YES - 5		
(c)	Receipt of false or stolen identification documents or information or refusal by Client to provide CDD documents.	NO - 0 YES - 5		
(d)	Client's project to be insured has no commercial / lawful rationale OR proposed transactions do not have an apparent economic / lawful purpose / sound commercial rationale	NO - 0 YES - 5		

(e)	Client has been convicted / sanctioned in relation to very serious crimes or offense or there is an ongoing case against the Policy Holder and/or its Board/Management and as a result, the business relationship cannot be accepted.	NO - 0 YES - 5		
(f)	None of the above If yes, please proceed with the rest of the Form	YES - 0		
	• TOTAL			

- **Scoring at least 5 under Part I results in outright rejection of the client.**

	RISK ASSESSMENT CRITERIA	GUIDE	SCORE	COMMENTS / RATIONALE
II.	**CLIENT RISK**	**(1)-(80) LR 0-5 MR 6-34 HR ≥ 35**	**RATING: /70 0**	**LOW MEDIUM HIGH**
1	**Politically Exposed Persons ('PEPs') or High Public Profile Individuals / UBOs; HNWIs**	**(0)– (10) LR (0) Ø HR >0**	**0**	
(a)	Any PEPs or Close Associates to PEPs or PEP involved in relationship or PEP links Any prominent position or enjoy a high public profile or HNWI that might enable them to abuse this position for private gain?	**Ø Yes (5) No (0)**		
(b)	Are any of the client's directors (if applicable) or service providers PEPs? Any political connections? Any other relevant links to a PEP? And, if so, do these PEPs exercise significant control over the client/beneficial owner? Or HNWI?	**Ø Yes (5) No (0)**		
Ø If PEP, former PEP or close associate of PEP, HNWI, client risk and overall rating becomes automatically HIGH and Board's Approval is sought for client acceptance				

2	**Type of Client / Controlling Person(s) of the Client**	**(1)– (15) LOW <5 HIGH>5**	**0**	
(a)	Individual	**(5)**		

(b)	i) Legal Person regulated in a Jurisdiction not sanctioned or called for action by FATF / Jurisdiction under increased monitoring as per FATF etc. ii) Legal Person regulated in a Jurisdiction called for action by FATF / Jurisdiction under increased monitoring as per FATF / High-risk jurisdiction µ / Others	**(0)** **(5)**		
(c)	Other Legal Arrangement or Structure? Charities or Non-Profit Organisations ("NPOs")	**(5)**		
3	**Source of Funds or Source of Wealth of the Client**	**(1)-(20)** **LR (1)** **MR (5)** **HR (10)**	**0**	**To define**
(a)	Client's source of funds or source of wealth established?	**Yes (0)** **No (10)**		
(b)	Nature of funds / Social / Financial Status of the Client	**LR (1)** **MR (5)** **HR (10)**		
4	**Independent Search Results (Screening or by other independent means)**	**(0)-(15)** **LR (0)** **MR = (5)** **HR > (5)**	**0**	
(a)	Convictions / sanctions / ongoing lawsuits / adversely commented press reports / public criticism, which relate to the client / BOs / UBOs/ Controller **(Φ)** and require close attention which EDD measures could not discount	**(5)**		
(b)	Past convictions or supervisory sanctions or enforcement for failure to comply with AML/CFT obligations or wider conduct requirements in recent years imposed on client which require close attention. Any other relevant Legal and Regulatory Issues?	**(5)**		
(c)	No screen searches or EDD conducted based on the documents provided by the Client?	**(5)**		
(Φ) Please see notes section w.r.t UBO / BO / Controller				

5	**Individual's Occupation / Legal Person's business / Legal Arrangement's or NPOs' Purpose**	**(1)– (20) LR (1) MR (5) HR ≥ 5**	**0**	
(a)	Links to sectors that are commonly associated with higher corruption risk, such as construction, pharmaceuticals and healthcare, the extractive industries or public procurement? *(Refer to business activity table at last page)*	**Yes (5) No (0)**		
(b)	Links to sectors that are associated with higher ML and/or TF risk, for example, certain money service providers ("MSPs"), casinos or dealers in precious metals or involve significant amounts of cash?	**Yes (5) No (0)**		
(c)	Business Activity of the Legal Person / Occupation of the Client / Purpose of the Legal Arrangement or NPO	**LR (1) MR (5) HR (10)**		

Refer to the NRA classification of different sectors in Notes Section for Part I (5)(c)

III.	**Products, Services and Transactions Risk**	**(3)– (30) LR = 4 MR 5-11 HR ≥ 12**	**RATING: /30 0**	
1	Level of transparency, including control over Client's bank account, availability of support documentation for transaction, transaction of the Client in line with business activity of the Financial Institution or opaqueness of the product, service or transaction	**LR (1) MR (3) HR (5)**		
2	Value or size of the transaction	**LR (1) MR (5) HR (10)**		
3	Any third party that is not part of the business relationship to give instructions? Any third-party payments unrelated to the business relationship?	**LR (0) HR (10)**		
4	Risks associated with new or innovative product or service, in particular where any use of new technologies or payment methods or is outside the field of expertise of the Company?	**LR (1) MR (3) HR (5)**		

	Countries / Territories and Geographical Areas Risk	(0)– (50) LR (0) MR (5-25) HR > 25	RATING: /50 0	
1	**Nationality of Individual / UBO / Controller**			
	International Tax Transparency and Information Sharing Standards / FATCA Participating Jurisdiction / CRS Committed Jurisdiction / Country's or Territory's ML/TF investigative judicial system / No sanctions	**LR (0)**		
	Non-Compliance with FATF 40 + 9 Recommendations / Weakness in Government Legislation to combat Money Laundering / Corruption Index (Transparency International & W.G.I) / World Governance Indicators (Political Issues)	**MR (5)**		
	Jurisdiction called for action by FATF / Jurisdiction under increased monitoring as per FATF / Others	**HR (10)**		

2	**The country in which the individual / UBO / Controller lives/is located?**			
	International Tax Transparency and Information Sharing Standards / FATCA Participating Jurisdiction / CRS Committed Jurisdiction / Country's or Territory's ML/TF investigative judicial system / No sanctions	**LR (0)**		
	Non-Compliance with FATF 40 + 9 Recommendations / Weakness in Government Legislation to combat Money Laundering / Corruption Index (Transparency International & W.G.I) / World Governance Indicators (Political Issues)	**MR (5)**		
	Jurisdiction called for action by FATF / Jurisdiction under increased monitoring as per FATF / Others	**HR (10)**		

3	**The country in which the individual / beneficial owner / UBO / Controller operates?**			
	International Tax Transparency and Information Sharing Standards / FATCA Participating Jurisdiction / CRS Committed Jurisdiction / Country's or Territory's ML/TF investigative judicial system / No sanctions	**LR (0)**		
	Non-Compliance with FATF 40 + 9 Recommendations / Weakness in Government Legislation to combat Money Laundering / Corruption Index (Transparency International & W.G.I) / World Governance Indicators (Political Issues)	**MR (5)**		
	Jurisdiction called for action by FATF / Jurisdiction under increased monitoring as per FATF / Others	**HR (10)**		

4	**Geographic location of source of Funds**			
	International Tax Transparency and Information Sharing Standards / FATCA Participating Jurisdiction / CRS Committed Jurisdiction / Country's or Territory's ML/TF investigative judicial system / No sanctions	**LR (0)**		
	Non-Compliance with FATF 40 + 9 Recommendations / Weakness in Government Legislation to combat Money Laundering / Corruption Index (Transparency International & W.G.I) / World Governance Indicators (Political Issues)	**MR (5)**		
	Jurisdiction called for action by FATF / Jurisdiction under increased monitoring as per FATF / Others	**HR (10)**		

5	**Destination of Funds**			
	International Tax Transparency and Information Sharing Standards / FATCA Participating Jurisdiction / CRS Committed Jurisdiction / Country's or Territory's ML/TF investigative judicial system / No sanctions	**LR (0)**		
	Non-Compliance with FATF 40 + 9 Recommendations / Weakness in Government Legislation to combat Money Laundering / Corruption Index (Transparency International & W.G.I) / World Governance Indicators (Political Issues)	**MR (5)**		
	Jurisdiction called for action by FATF / Jurisdiction under increased monitoring as per FATF / Others	**HR (10)**		

	Delivery Channels Risk	**(1)– (20)** **LR 1** **MR 5** **HR ≥ 10**	**RATING: /20**	
1	Frequent Face-to-face Client Relationship, including video	**(1)**		Specify Frequency (wherever applicable)
2	Only non-face-to-face* Client Relationship (including mail, phone, text, internet) and/or via Intermediary, including Gatekeepers ** If a client is known to the FI but conducts their business activity non-face-to-face, then Moderate Risk.*	**MR (5)** **HR (10)**		
3	Unsolicited Client Relationship (including walk-ins)	**(20)**		

VI.	**Consistency/Completeness of Information**	**(0)– (20)** **LR 0** **MR 5-10** **HR > 10**	**RATING: /20** **0**	

1	Outstanding Basic KYC / CDD Documents Outdated KYC / CDD Documents All CDD documents obtained	**(10)** **(5)** **(0)**		
2	Any additional relevant factor(s) to take into consideration?	**(5)**		
	TOTAL RATING	**(200)**	**0**	

COMMENTS:

RISK ASSESSMENT SUMMARY

	Client Risk / Nature, Scale & Complexity of Client Activities PART II	Product, Services and Transactions Risk PART III	Countries / Territories and Geographical Areas Risk PART IV	Delivery Channels Risk PART V	Consistency / Completeness of Information PART VI	OVERALL RISK
ACCEPT & REVIEW						
PEP	HIGH					**HIGH**

Prepared by:	**Signature:**	**Date:**
Reviewed by:	**Signature:**	**Date:**

Overall Risk Level	Overall Risk Rating
Low	0 - 59
Medium	60 - 129
High[1]	130 - 200

[1]In the event where a client file is categorized as high risk, Enhanced Due Diligence (EDD) measures should be applied in accordance with Regulation 12(1) of the FIAML Regulations 2018 and Chapter 6 of the FSC AML/CFT Handbook 2020.

APPROVED BY CLIENT ACCEPTANCE COMMITTEE[2]/CO/MLRO

Signature:

Compliance Officer / MLRO **Managing Director/CEO**

Date:

[2]wherever applicable, particularly for new clients being on-boarded

Low
Medium
High

Notes:

μ: High-Risk Jurisdiction

To assess whether a jurisdiction is a High-Risk jurisdiction, due consideration shall be given to:

- FATF High-risk and other monitored jurisdictions
- **European Commission** AML/CFT List of High Risk Third Countries
- **European Commission's** list of non-cooperative jurisdictions for tax purposes
- Transparency International's Annual Corruption Perceptions Index
- **OECD** Global Forum on Tax Transparency and Exchange of Information for Tax Purposes Ratings
- **Office of Foreign Affairs Control (OFAC)** Countries List
- **Basel** AML Index
- Corruption Perception Index
- Global Peace Index
- Global Terrorism Index
- Financial Secrecy Index
- Run through "Know Your Country" FATF AML Deficiency List & Use "Google Boolean"

Business Activity Classification:

a) List of activities classified as High Risk:

1. Extractive Industries: Entities that deal in the extraction of natural resources, such as oil, minerals, gas and timber.
2. Government/Public Procurement Activities
3. Defence Industry: Contracting Work of highly specialised goods, systems and services.
4. Human Health Activities: Provision of health services, pharmaceutical products, and medical devices, including research, development, dispensing and promotion of same.
5. Large Infrastructure Projects: Contracting work for construction, continuing maintenance and upkeep.
6. Privatisation: Buying or obtaining from government something of large economic value through the process of privatisation.
7. Activities related to so-called "windfall revenue" including significant amounts of foreign aid.
8. FX Trading
9. Jewels, gems and precious metal dealers
10. Real estate agents
11. Cash Pooling Structures
12. Virtual currency trading (e.g. bitcoins)
13. Dealing in cultural objects like in sculpture, statues, antiques, collector items, archaeological

pieces

14. NGO's and NPO (Non-profit organization)
15. Online trading/online marketing and E-commerce
16. Activities in gambling sector and casinos
17. Money Service provider
18. Trust and Company service Provider

b) List of activities classified as Medium Risk:

1. Legal Professions (including Law firms/ Barristers, Notaries, attorneys)
2. Accountancy sector (including Accounting firm and Auditors)
3. Trust and Company service Provider
4. Consultancy
5. Trading (e.g. Import and Export)
6. Life Insurance Sector
7. Banking Sector
8. Financial Institutions regulated by the FSC
9. Non-financial Entities regulated by the FSC
10. Financial Institutions regulated by BOM
11. Credit Union
12. Securities sector

c) List of activities classified as Low Risk:

1. Public Listed Companies on stock exchange
2. International Organisation (e.g. United Nation)
3. Government administrations or enterprises and statutory bodies

NRA Report 2019 :

https://financialservices.govmu.org/Documents/NRA%20Report/Public%20Report%202019-compressed.pdf

Appendix 7: PEP Declaration Form & PEP Register

DECLARATION OF POLITICALLY EXPOSED PERSON STATUS FORM

Please answer the questions/state the information requested below with regards to Politically Exposed Person ("PEP"). This is to enable the Company to comply with its obligations pursuant to the Financial Intelligence and Anti-Money Laundering Act 2002 relating to measures to combat money laundering and the financing of terrorism.

1. Do you currently hold, or have you been entrusted in the past with a prominent public function (1), or are you an immediate family member (2), or close associate (3) of such a PEP?

   ☐ No ☐ Yes - If yes, please specify (functions held, when and for how long, etc...)

   _____

   _____

<u>Origin of the funds/ wealth</u>

2. If you have answered ''Yes'' to the question above, the origin of any current, and the expected origin of any future funds/wealth, must be provided

   ☐ Business operations ☐ Returns on investments

   ☐ Loans ☐ Salaries

   ☐ Inheritance ☐ Other (Please specify)

_____

I/We hereby confirm that the above-stated information is correct and complete.
I/We undertake to promptly inform you, in writing, if there is any change in the status as declared above.

Signature: _____

Client's/Principal's name: _____

For and on behalf of

Date:

PEP REGISTER

	PEP NAME	NATIONALITY & PASSPORT ID	ENTITY IN WHICH THE PEP IS INVOLVED & POSITION HELD IN ENTITY	ENTITY ACTIVE OR INACTIVE	HITS OR ADVERSE MEDIA REPORT (IF ANY)	SCREENING DATES (CONDUCTED ON RISK BASIS)	COMMENTS
1.							
2.							
3.							
4.							
5.							
6.							
7.							

Appendix 8: Training Log

TRAINING REGISTER						
S/N	DATE	ATTENDEE(S)	TOPIC	TRAINING INSTITUTION	DURATION (HOURS)	CIML ANNUAL CPD AS AT NOW
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
DIRECTORS, CO & MLRO/DMLRO & Dealing Team						
Directors						
1						
2						
3						
4						
CO & MLRO/DMLRO						
1						
2						
3						
4						
5						
6						
Dealing Teams						
1						
2						
3						
4						
5						

Appendix 9: Internal STR Log

Internal Suspicious Transactions Report (iSTR)

Internal Disclosure Form to MLRO

1. Reporting Employee;
Name:
Telephone No:

2. Customer Details;
Client Name:
Address:
Contact Name:
Contact Telephone No:
Date Business Relationship Commenced:
Customer reference:

3. Information/Suspicion
Suspected Information/Transaction:
Reasons for Suspicion:
Please attach copies of any relevant documentation to this report.

Reporter's Signature: **Date:**

It is an offence to advise the Customer or anyone else of your suspicion and report. This report will be treated in the strictest confidence.

For MLRO Use:		
Date received: ……..	Time received: ……	Ref:…….
FIU advised …. Yes/No	Date: ……..	Ref:

Appendix 10: Adverse Media / Compliance Reports

The Investment Dealer has outsourced the screening function to its Management Company which uses an automated screening engine. The engine may come across Adverse Media and / or hits in the following circumstances:

- Upon verifying the trust worthiness of a client during the client acceptance phase.
- After the client has been accepted, as part of the ongoing monitoring of the client.

In both circumstances, the Compliance Officer/MLRO (or DMLRO in the latter's absence) shall prepare a compliance report, including therein his recommendations, and submit to the Board, which shall resolve on the next course of action.

The report shall be signed off by the Compliance Officer/MLRO (or DMLRO in the latter's absence) and a director of the Investment Dealer before being submitted to the FSC.

Appendix 11: Updated CDD Documents

As part of the ongoing monitoring of clients, the Company shall:

- Monitor the expiry of passports of clients and request for renewed passports as and when necessary, thus ensuring that copies of valid passports, incorporating photographic evidence of identity, are held by the Company at all times.

- Where it becomes aware of a particular aspect of the client's identity has changed (e.g., change of name, nationality, or any other forms as approved), gather relevant updated CDD documents.

- Request clients for updated proof of address under the following risk-based approach, i.e., request frequency shall be based on the risk classification of clients.

Risk level	**Frequency to confirm validity of the Address***	**Frequency to seek updated Proof of Address**
Low risk	Annually	Every Three Years
Medium risk	Annually	Every Two Years
High risk	Bi-Annually	Annually

*The confirmation of the validity of the Address shall be in the form of email.

Appendix 12: Acknowledgement Form

Acknowledgement Form

I .....(name of employee) acknowledge having had sufficient time to read and understand the content of this Compliance Manual. I also acknowledge having had the opportunity to ask questions or raise any query I may have had with the Company's Compliance officer and Money Laundering Reporting Officer.

I further agree to adhere to the policies, principles, procedures and processes as laid down in the Compliance Manual, including in the policies, procedures and processes attached thereto, and acknowledge that the Company may take relevant actions/apply sanctions in case of non-compliance with the Manual or any other process, policy or procedure of the Company.

(Please write 'Read and Understood' in own handwriting)

Signature of Employee

Name of Employee:……

Date:

Appendix 13: Source of Fund Declaration Form

NAME OF COMPANY	
Verification of Source of Funds & Wealth	
Full Name / Legal Name:	
Identity No/ Company No:	
Nationality/Country of Incorporation:	
Date of Birth /Date of Incorporation:	
Permanent Residential/ Business Address:	
Telephone No:	
Email:	

I/We hereby confirm that deposits made into the Company:

1. Are not made on behalf of a third party; and
2. The funds deposited are derived from legitimate source and are not linked and/or derived from criminal origin, of whatsoever nature, and in particular do not constitute the proceeds of Money Laundering and Terrorist Financing.

Confirmation on Politically Exposed Persons (''PEP'')

(Check "✓" all that apply)

PEP ☐ PEP-Related ☐ Not Applicable

Source of Funds Declaration - Full description of source of funds to be deposited.

Source of Funds: (Check "✓" all that apply)

1. Capital of Company ☐
2. Income from Salary ☐
3. Dividends ☐
4. Income from Business operations ☐
5. Gift ☐
6. Inheritance ☐
7. Profit from sale or maturing Investments ☐
8. Profit from Property sale ☐
9. Income from Sale of Company shares ☐
10. Fixed Deposit Savings ☐
11. Other, (please specify) ☐ ……...

Name of remitting bank:
Address of remitting bank:
Remitter Account Name:
Remitter Account Number:
Other details:

Origin of Wealth
Origin of Wealth: (Check "✓" all that apply) 1. Income from Salary ☐ 2. Maturity or surrender of Life Insurance Policy ☐ 3. Sale/Liquidation of Investment ☐ 4. Sale of Property ☐ 5. Company Sale ☐ 6. Inheritance ☐ 7. Divorce Settlement or any other form of settlement compensation ☐ 8. Company profits ☐ 9. Retirement Income ☐ 10. Dividend/Royalties Payment ☐ 11. Employment ☐ 12. Rental Income ☐ 13. Other, (please specify) ☐ ……...

Acknowledgment and Certification
We/I acknowledge that it is the policy of the XXX to verify the source of funds deposited into the Client Segregated Account and hereby certify that the funds deposited are derived from the sources above. The funds are not / will not be derived from or otherwise be connected with any activity which is illegal or unlawful, either in their country of origin or in any other location associated with this account. We/I will provide the required evidence of the source of funds on funds deposited now and/or otherwise required to doing so in future. We/I further confirm that the transfer of assets to XXX are not in breach of any money laundering regulations and laws applicable to the Republic of Mauritius, including but not limited to the Financial Intelligence and Anti-Money laundering Act 2002 and 2018 and the Prevention of Terrorism Act 2002. **DONE IN GOOD FAITH AND AFTER DUE CONSIDERATION.**

Signature	

Appendix 14: List of Rejected Clients

Company Name				
List of Rejected Clients				
Client Name	Related Company (if applicable)	Date of Rejected	Reasons for Rejecting Client	Has FSC been informed? (if applicable)

Appendix 15: Management of Interest Policy & Register of Interest

What is an interested transaction?

Section 147 of the Companies Act 2001 defines "interest in a transaction" as one to which the company is a party where the director –

(a) is a party to, or shall or may derive a material financial benefit from the transaction;

(b) has a material financial interest in or with another party to the transaction;

(c) is a director, officer, or trustee of another party to, or person who shall or may derive a material financial benefit from, the transaction, or being a party or person that is –

(i) the company's holding company being a holding company of which the company is a wholly-owned subsidiary;

(ii) a wholly-owned subsidiary of the company; or

(iii) a wholly-owned subsidiary of a holding company of which the company is also a wholly-owned subsidiary;

(d) is the parent, child or spouse of another party to, or person who shall or may derive a material financial benefit from, the transaction; or

(e) is otherwise directly or indirectly materially interested in the transaction.

Section 147(2) of the Companies Act 2001 further clarifies that a director of a company shall not be deemed to be interested in a transaction to which the company is a party if the transaction comprises only the giving by the company of security to a third party and at the request of that third party which has no connection with the director and in respect of a debt or obligation of the company for which the director or another person has personally assumed responsibility in whole or in part under a guarantee, indemnity, or by the deposit of a security.

Banning these transactions is normally not a solution as there is nothing wrong per se with entering into transactions with related parties provided the conflict of interest inherent in these transactions are adequately addressed including through proper monitoring, approval and disclosure to avoid potential abuse of related party transactions.

Disclosure of conflict of interest

Section 148 of the Companies Act 2001 and Principle 4 of the National Code of Corporate Governance 2016 relating to Director Duties, Remuneration and Performance provide that a director of a company shall, forthwith after becoming aware of the fact that he is interested in a transaction or proposed transaction with the company, cause to be entered in the interests' register, where it has one, and, where the company has more than one director, disclose to the Board of the company –

(a) where the monetary value of the director's interest is able to be quantified, the nature and monetary value of that interest; or

(b) where the monetary value of the director's interest cannot be quantified, the nature and extent of that interest.

However, a director of a company is not required to make the above disclosures where -

(a) the transaction or proposed transaction is between the director and the company; and

(b) the transaction or proposed transaction is or is to be entered into in the ordinary course of the company's business and on usual terms and conditions.

How to make disclosure?

A general notice is entered in the interests register or disclosed to the Board to the effect that a director is a shareholder, director, officer or trustee of another named company or other person and is to be regarded as interested in any transaction which may, after the date of the entry or disclosure, be entered into with that company or person, is a sufficient disclosure of interest in relation to that transaction.

A Register of Interest is provided below for the implementation.

Failure to disclose

A failure by a director to disclose any potential conflict of interest shall not affect the validity of a transaction entered into by the company or the director.

Avoidance of transactions

Section 149 of the Companies Act 2001 further clarifies the following:

A transaction entered into by the company in which a director of the company is interested may be avoided by the company at any time before the expiration of 6 months after the transaction is disclosed to all the shareholders whether by means of the company's annual report or otherwise.

A transaction shall not be avoided where the company receives **fair value** under it.

(a) The question as to whether a company receives a fair value under a transaction shall be determined on the basis of the information known to the company and to the interested director at the time the transaction is entered into.

(b) Where a transaction is entered into by the company in the ordinary course of its business and on usual terms and conditions, the company shall be presumed to have received a fair value under the transaction.

(c) A person seeking to uphold a transaction and who knew or ought to have known of the director's interest at the time the transaction was entered into shall have the onus of establishing a fair value; and

(d) In any other case, the company shall have the onus of establishing that it did not receive a fair value.

A transaction in which a director is interested shall only be avoided on the ground of the director's interest in accordance with this section or the company's constitution.

To whom does this interest policy apply?

This policy is to be strictly followed by all officers, including directors, shareholders, officers, or trustees of the Company, as may be applicable, in view of the nature of the business of the Company.

Company XXX

REGISTER OF INTERESTS

Type: Investment Dealer (Full-Service Dealer, Excluding Underwriting) License (Pursuant to Section 29 of the Securities Act 2005)

Date of Incorporation: XXX XXX XXX

Company number: CXXX GBC

Date of Appointment	Position	Name of Member	Description of Interest
	Ultimate Beneficial Owner		**Mr. XX is the Ultimate Beneficial Owner of the Company.** He owns 100% shares of the Company. He has full ownership and ensure that the company comply with its obligations.
	Non-Resident Director		**Mr. XX is the director of the Company.** He participates in board meetings to enable the board to reach certain decisions ensuring that the company's obligations are fulfilled.
	Non-Resident Director		**Mr. XX is the director of the Company.** He participates in board meetings to enable the board to reach certain decisions ensuring that the company's obligations are fulfilled.
	Resident-Director		**Mr. XX is the director of the Company.** He participates in board meetings to enable the board to reach certain decisions ensuring that the company's obligations are fulfilled.
	Resident-Director		**Mr. XX is the director of the Company.** He participates in board meetings to enable the board to reach certain decisions ensuring that the company's obligations are fulfilled.
	Head of Dealing		**Mr. XX is the Head of Dealing of the company.** He monitors company margin levels at the liquidity providers. Also, he ensures trading infrastructure is secure and working smoothly. He adheres to the in-house Code of Ethics which forms part of employment contract, and which

			includes the following key policies: Management of Conflict of Interest, Confidentiality of Client and Business information, Provision of Receipt of Gifts or Events or other benefits.
	Assistant Head of Dealing		**Mr. XX is the Assistant Head of Dealing of the company.** He configures and administer trading systems, including XXX. Also, he formally presents recommendations and solutions for any issues to the senior management team based on analysis of data. He also document operations and risk management procedures and policies and manage internal knowledge sharing site.
	DMLRO		**Mrs. XXX is the CO & MLRO of the Company.** As a DMLRO, She is responsible to receive internal disclosures in the absence of the MLRO and determine whether and an external disclosure is required .
	CO/MLRO		**Mr. XXX is the MLRO of the Company.** As a CO, he is responsible for ensuring continued compliance with the requirements of FIAMLA and FIAML Regulations 2018 and having an overall oversight of the program for combatting money laundering and terrorism financing amongst others (Regulation 22(3) of FIAML Regulations 2018). Also, as a MLRO, he is responsible to design and implement and update the manuals as required. He also review and examine the internal disclosures and determine if the transaction reports are suspicious and reporting must be made to the FIU.

Name:

Designation: Company Secretary / Director

Date:

Signature:

Appendix 16: Third Party Risk Assessment Template

THIRD PARTY RISK ASSESSMENT

XXX

(the "Company")

Name of Service Provider:	XXX
Overall Risk Rating:	XXX / 100
Overall Risk Level:	Low Risk ('LR') ☐ Medium Risk ('MR') ☐ High Risk ('HR') ☐
Date of Risk Assessment:	XXX
Date of Next Review:	XXX

	Risk Assessment Criteria	Inherent Risk Rating Guide	Likelihood Risk Rating	Comments | Mitigating Controls
I.	**Client Risk**			
1.	**Type of Service Provider**			
	Individual	**(5)**		
	Legal Person regulated in a Jurisdiction not sanctioned or called for action by FATF / Jurisdiction under increased monitoring as per FATF	**(0)**		
	Legal Person regulated in a Jurisdiction called for action by FATF / Jurisdiction under increased monitoring as per FATF / High-risk jurisdiction µ / Others	**(5)**		
2.	**Nature of Business**			
	Products / Services offered (refer to Annex 1 – *Methodology: Business Activity Classification*)	**LR (1)** **MR (3)** **HR (5)**		
II.	**Countries / Territories and Geographical Risk**			
1.	**Country of Incorporation / Nationality of the Service Provider**			
	International Tax Transparency and Information Sharing Standards / FATCA Participating Jurisdiction / CRS Committed Jurisdiction / Country's or Territory's ML/TF investigative judicial system / No sanctions	**LR (0)**		
	Non-Compliance with FATF 40 + 9 Recommendations / Weakness in Government Legislation to combat Money Laundering / Corruption Index (Transparency International & W.G.I) /	**MR (5)**		

	World Governance Indicators (Political Issues)			
	Jurisdiction called for action by FATF / Jurisdiction under increased monitoring as per FATF / Others	**HR (10)**		
2.	**The country in which the Service Provider lives/operates/is located)**			
	International Tax Transparency and Information Sharing Standards / FATCA Participating Jurisdiction / CRS Committed Jurisdiction / Country's or Territory's ML/TF investigative judicial system / No sanctions	**LR (0)**		
	Non-Compliance with FATF 40 + 9 Recommendations / Weakness in Government Legislation to combat Money Laundering / Corruption Index (Transparency International & W.G.I) / World Governance Indicators (Political Issues)	**MR (5)**		
	Jurisdiction called for action by FATF / Jurisdiction under increased monitoring as per FATF / Others	**HR (10)**		
3.	**Destination of funds**			
	International Tax Transparency and Information Sharing Standards / FATCA Participating Jurisdiction / CRS Committed Jurisdiction / Country's or Territory's ML/TF investigative judicial system / No sanctions	**LR (0)**		
	Non-Compliance with FATF 40 + 9 Recommendations / Weakness in Government Legislation to combat Money Laundering / Corruption Index (Transparency International & W.G.I) / World Governance Indicators (Political Issues)	**MR (5)**		
	Jurisdiction called for action by FATF / Jurisdiction under increased monitoring as per FATF / Others	**HR (10)**		
III.	**Independent Search Results (Screening or by other independent means)**			
	Politically Exposed Person (PEP) / PEP involved in relationship / PEP links	**Ø Yes (5)** **No (0)**		
	Convictions / sanctions / ongoing lawsuits / adversely commented press reports / public criticisms	**Ø Yes (5)** **No (0)**		
IV.	**Technological Risks**			
	Risks associated with the product or service, in particular where any use of new technologies or payment methods or is outside the field of expertise of the Company?	**LR (1)** **MR (3)** **HR (5)**		
V.	**Customer Due Diligence (CDD)**			
	All CDD documents obtained Outdated KYC / CDD documents Outstanding Basic KYC / CDD documents	**LR (0)** **MR (2)** **HR (10)**		

VI.	**Any additional relevant factor(s) to take into consideration?**	**(5)**		
	Total Rating	**(100)**		

Comments:

Overall Risk level	**Overall Risk Rating**	**Frequency of Review Screening**
Low Risk (LR)	0 - 25	Every 3 Years
Medium Risk (MR)	26 - 40	Every 2 Years
High Risk (HR)*	41 - 100	Yearly

**In the event where a is categorized as high risk, Enhanced Due Diligence (EDD) measures should be applied in accordance with Regulation 12 of the FIAML Regulations 2018 and Chapter 6 FSC Handbook.*

Approval of the Board of Directors / Compliance Officer / MLRO is warranted.

Prepared by:	XXX | Compliance Analyst
Date:	
Signature:	
Reviewed & Approved by:	XXX | Compliance Officer
Date:	
Signature:	

ONGOING MONITORING – THIRD PARTY RISK ASSESSMENT

ONGOING RISK ASSESSMENT – HAVE ANY RISK FACTORS CHANGED?	LOW ☐	MEDIUM ☐	HIGH ☐
Please state your assessment:			
Prepared by:	Date:	Signature:	
Reviewed & Approved by:	Date:	Signature:	

ONGOING RISK ASSESSMENT – HAVE ANY RISK FACTORS CHANGED?	LOW ☐	MEDIUM ☐	HIGH ☐
Please state your assessment:			
Prepared by:	Date:	Signature:	
Reviewed & Approved by:	Date:	Signature:	

Appendix 17: Transaction Monitoring Template

Company Name	
Type	
Bank Name	
Currency	
Account number	
Task	

SR No.	Date	Inwards Amount	Outwards Amount	Details of Remitter	Purpose of Payments	Supporting documents	In Line with Business	KYC documents on Remitters	Compliance Verifications		Remarks
									World Check	Internet Search	
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											
11											
12											
13											
14											
15											
16											
17											
18											
19											
Date:						Date:					
Prepared by:						Reviewed by:					
Signature:						Signature:					