HIGHNESS INVESTMENT LLC
AML/CFT MANUAL

TABLE OF CONTENTS

Page

CHAPTER 1: INTRODUCTION

a) Overview of the Company

HIGHNESS INVESTMENT LLC (the "Company") is a private company limited by shares in accordance with the Mauritius Companies Act 2001.

The Company is therefore accountable to the FSC in terms of compliance with the law and with the term of its license.

Due to the nature of its activities, the Company understands that the Company might be exposed to Money Laundering, Terrorist Financing, and Proliferation of Weapons of Mass Destruction Schemes.

It is committed to maintaining the highest degree of diligence in the choice and management of its business.

The Company believes that the key to the prevention of Money Laundering and Terrorist Financing is the implementation of and adherence to proper compliance procedures (effective identification 'KYC' and diligence procedures) both at the beginning of every relationship and on an ongoing basis thereafter.

Adequate compliance procedures, both in the acceptance of a client and on an ongoing basis, should enable the Company to know its clients enough and their activities. Therefore, unusual or unexpected activity can be recognized when or before it occurs, and the identification and management of risks inherent in certain client relationships.

b) Purpose of this Manual

This AML/CFT Manual (the "Manual") details the procedures – must followed by all employees of the Company to ensure compliance with the various Guidelines, and legal requirements.

The FSC issued an Anti-Money Laundering and Countering the Financing of Terrorism Handbook (the Handbook) on the 13th of January 2020 which has been amended on 31 March 2021. The Handbook has been designed to aid the Company in complying with obligations contained within the relevant legislations. The Handbook is designed to serve as a statement of minimal criteria, describe Anti Money Laundering practice expected from the Company, and scrutinise each relationship and transaction with a risk-based approach, not a rule-based approach. Non-observance of the Handbook under relevant legislative provisions may result in revocation of the Company's license. This Manual reflects inter alia the requirements of the Handbook.

c) Application of this Manual

The contents of this Manual apply to all employees of the Company including but not limited to the directors, authorised individuals, managers, executives and interns of the Company, whether employed full time or part time, directly or indirectly.

In this Manual, "the Company", "we", "our" or "us" may refer or any subsidiaries and affiliates (and its respective successors in title).

The Board of Directors of the Company (the "Board") is ultimately responsible for compliance with the contents of this Manual.

The Board has delegated the day-to-day responsibility for their implementation to the Compliance Officer (CO).

d) Objectives of this Manual

The objective of this AML/CFT (the "Manual") is to ensure that the services offered by the Company are not used to launder proceeds of crime and that all of the Company's staff are aware of their obligations and the need to remain vigilant in the fight against money laundering/terrorist financing. The Manual also provides a framework to comply with applicable laws, regulatory guidelines specially related with detection and reporting of suspicious transactions.

Under the Financial Intelligence and Anti-Money Laundering Act 2002 (''FIAMLA''), the Company is required to establish appropriate risk-sensitive policies and procedures in order to prevent activities related to money laundering and terrorist financing including those policies and procedures which provide for:

- identification and scrutiny of complex or unusual patterns of transactions with no apparent economic or lawful purpose and other activities regarded by the regulated person as likely to be of the nature of money laundering or terrorist financing;

- prevention of use of products favoring anonymity;

- determination of whether a client is a PEP;

- customer due diligence, i.e., procedures designed to acquire knowledge about the Company's clients and prospective clients and to verify their identity as well as monitor business relationships and transactions;

- internal reporting including appointment of a Money Laundering Reporting Officer (''MLRO'') and a Deputy Money Laundering Reporting Officer (''DMLRO'') to receive the money laundering reports required under the Proceeds of Crime Act 2002 (POCA) and the Terrorism Act 2000 (TA) and a system for making those reports;

- designate a CO to be responsible for the implementation and the ongoing compliance of the Company with internal programs, controls and procedures with the requirements of FIAMLA and FIAML Regulations;

- record keeping, including details of customer due diligence and supporting evidence for business relationships, which need to be kept for seven years after the end of a relationship and records of transactions, which also need to be kept for seven years;

- internal control, and management, compliance monitoring, management and communication; and

- in addition, the Company shall take measures to make relevant employees aware of the law relating to money laundering and terrorist financing, and to train those employees on how to recognize and deal with transactions which may be related to money laundering or terrorist financing.

In order to ensure compliance is appropriately managed, the Company shall ensure sufficient senior management oversight, appropriate analysis and assessment of the risks of clients and work/product types, systems for monitoring compliance with procedures and methods of communicating procedures and other information to personnel.

e) Scope of the Manual

The Manual encompasses and adheres to the following:

- The Financial Intelligence and Anti-Money Laundering Act 2002 ("FIAMLA")

- The Financial Intelligence and Anti-Money Laundering Regulations 2018 ("FIAML Regulations")

- The Anti-Money Laundering and Countering the Financing of Terrorism Handbook (the 'Handbook')

- The FATF Recommendations

This AML/CFT Policy is a methodology that defines how the Company monitors accounts, detects and reports financial crimes to relevant authorities. Essentially, this Policy tackles the inherent and residual money laundering risks the Company faces.

The Board of the Company has duly approved the content of this Manual and the following core principles:

- Application of Customer Due Diligence measures prior to establishing any business relationship with clients;

- Appointment of Compliance Officer, Money Laundering Reporting Officer (MLRO) and Deputy MLRO and their roles and functions;

- Risk-based approached and risk profiling procedures;

- Implementation of effective on-going Customer Due Diligence (CDD) measures;

- Provision of AML/CFT trainings to new staff and on-going training to existing staff;

- Procedures for monitoring of transactions and activity;
- Policies and procedures for reporting of Suspicious Transactions to the FIU;
- Implementation and maintenance of effective record keeping systems.

CHAPTER 2: LEGISLATIVE FRAMEWORK: LAWS AND INSTITUTIONS

a) Financial intelligence and Anti-Money Laundering Act 2002 ("FIAMLA")

The primary statute governing money laundering offences is the Financial Intelligence and Anti-Money Laundering Act 2002 ("FIAMLA") which has been amended in 2019 to broaden the scope of preventive measures to be consistent with the Financial Action Task Force' standards.

b) Financial Intelligence and Anti Money Laundering Regulations 2018 ("FIAML Regulations 2018")

The FIAML Regulations 2018 were promulgated on 28 September 2018 and became effective on 01 October 2018. The Regulations 2018 revoked the Financial Intelligence and Anti-Money Laundering Regulations 2003 and address, inter alia, the following FATF requirements:

(a) Customer Due Diligence;

(b) Politically exposed persons;

(c) Correspondent banking;

(d) Money or value transfer services;

(e) New technologies;

(f) Wire transfers;

(g) Reliance on third parties; and

(h) Internal control and foreign branches and subsidiaries.

c) FSC Anti-Money Laundering and Countering the Financing of Terrorism Handbook (The "Handbook")

The purpose of the Handbook is to assist and provide guidance to financial institutions to comply with the requirements of all relevant legislation pertaining to money laundering and terrorism financing, financial crimes and other related offences. A "financial institution" is defined in the FIAMLA as an institution, or a person, licensed or registered or required to be licensed or registered under section 14, 77, 77A or 79A of the Financial Services Act 2007, the Insurance Act 2005, the

Securities Act 2005, or the Captive Insurance Act 2015.

The Handbook emphasizes on the risk-based approach to be adopted by financial institutions for implementation of measures that correspond with the potential risks that may be identified in the business, providing an overview of money laundering, terrorist financing and proliferation offences, highlighting the importance of appointing a compliance officer, a money laundering reporting officer and a deputy money laundering reporting officer as part of good corporate governance and compliance with AML/CFT laws in Mauritius and setting out the minimum CDD requirements, as well as enhanced and simplified due diligence procedures that are applicable to financial institutions.

The purpose of the Handbook is to illustrate and provide examples of best practice and assist financial institutions in complying with AML/CFT laws. Although the Handbook is for guidance purposes, the FSC will consider the Handbook when assessing the level of compliance to the FIAMLA and, the Regulations.

d) 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 2019 amended various enactments with a view to meeting international standards of the Financial Action Task Force on anti-money laundering and combatting the financing of terrorism and activities related to the proliferation of weapons of mass destruction, and to provide for matters related thereto.

e) The Anti-Money Laundering and Combatting the Financing of Terrorism and Proliferation (Miscellaneous Provisions) Act 2020

The Anti-Money Laundering and Combatting the Financing of Terrorism (Miscellaneous Provisions) Act 2020 was enacted on 9 July 2020. The Act amended various enactments in view of furthering fundamental reforms in the financial services sector, thereby ensuring closer compliance with recommended international best practices and norms of the FATF. Accordingly, these measures aim to reinforce the existing legal provisions to further combat money laundering and the financing of terrorism.

f) The United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 ("Sanctions Act")

Pursuant to the Finance (Miscellaneous Provisions) Act 2018 passed in July 2018 in the Mauritius National Assembly, various enactments such as the existing Financial Intelligence and Anti-Money Laundering Act ("FIAMLA") 2002, the Financial Services Act ("FSA") 2007 and others have been amended with a view to align with international standards of the Financial Action Task Force on anti-money laundering and combating terrorism financing.

In addition, a new Act, namely the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 came into effect in May 2019.

This new United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 enables the Government of Mauritius to implement targeted sanctions, including financial

sanctions, arms embargo and travel ban, and other measures imposed by the United Nations Security Council under Chapter VII of the Charter of the United Nations, with a view to addressing threats to international peace and security, including terrorism, the financing of terrorism and proliferation of weapons of mass destruction.

g) The Financial Services Commission (Mauritius)

The Financial Services Commission, Mauritius (the 'FSC') is the integrated regulator for the non-bank financial services sector and global business. Established in 2001, the FSC is mandated under the Financial Services Act 2007 and has as enabling legislations the Securities Act 2005, the Insurance Act 2005 and the Private Pension Schemes Act 2012 to license, regulate, monitor and supervise the conduct of business activities of The Company as a licensee of the FSC conducting businesses in the financial non-banking sector as well as the global business sector.

h) The Financial Intelligence Unit

The Financial Intelligence Unit was established under section 9 of the FIAMLA. It is the central Mauritian agency for the request, receipt, analysis and dissemination of financial information regarding suspected proceeds of crime and alleged money laundering offences as well as the financing of any activities or transactions related to terrorism to relevant authorities. The FIU has been a member of the Egmont Group of Financial Intelligence Units since 2003. Cooperation with other Egmont members as well as other counterparts is highly valued by the FIU.

The Company under the FIAMLA and FIAML Regulations 2018 is a reporting person registered with the FIU for the purposes of reporting Suspicious transactions to this agency. The Company is committed to report any suspicious transactions it comes across in its daily operations to the FIU with the aim to combat money laundering and the financing of terrorism.

i) National Sanctions Secretariat (The “NSSec”)

The NSSec, established under the Sanctions Act, is the focal point for UN sanctions related matters, including coordinating and promoting effective implementation of the obligations under the UNSC resolutions in Mauritius. Under the Sanctions Act, the NSSec has the responsibility to immediately give public notice of any changes to any UN sanctions lists. This includes new designations, changes to existing designations, and removed designations. Furthermore, if a true match is identified by a reporting person, it must immediately submit a report to the National Sanctions Secretariat, and in some cases also to its relevant supervisory authority.

The NSSec supports the work of the of the National Sanctions Committee, and its objectives are the following:

- To issue such guidelines and disseminate such other relevant information as may be necessary for the effective implementation of the UN Sanctions Act;

- To facilitate the sharing of information with other agencies for the purposes of the Act;

- To collect or solicit information from public sector agencies and any party that is reasonably believed to hold, control or has in his or its custody or possession funds or other assets of a listed party;

- To enter into an arrangement or agreement with the Office of the Ombudsperson to facilitate the sharing of information, including confidential information;

- To keep and maintain, in such form and manner as the National Sanctions Committee may determine, a list of designated parties;

- To maintain a website with publicly available information relating to the Act;

- To publish information on relevant procedures for the purposes of the Act;

- To attend to the request forwarded by the Ministry of Foreign Affairs for a determination by the National Sanctions Committee as to whether there are reasonable grounds to declare the party as a designated party;

- To take such measures in accordance with the relevant United Nations Security Council Resolution for the removal of his name as a listed party from the relevant United Nations Sanctions List;

- To keep and maintain a list of funds or other assets frozen pursuant to a freezing order granted under the Act

j) The Eastern and Southern Africa Anti-Money Laundering Group (The "ESAAMLG")

The Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) was officially established in 1999 in Arusha, Tanzania through a Memorandum of Understanding (MOU). ESAAMLG membership comprises of 18 countries and includes several regional and international observers such as AUSTRAC, COMESA, Commonwealth Secretariat, East African Community, Egmont Group of Financial Intelligence Units, FATF, GIZ, IMF, SADC, United Kingdom, United Nations, UNODC, United States of America, World Bank and World Customs Organization. ESAAMLG's members and observers are committed to the effective implementation and enforcement of internationally accepted standards against money laundering and the financing of terrorism and proliferation, particularly, the FATF Recommendations.

Mauritius is a member of ESAAMLG, the assessment of the implementation of anti-money laundering and counter-terrorist financing (AML/CFT) measures in Mauritius was conducted by the International Monetary Fund (IMF) and adopted by ESAAMLG. Mauritius is evaluated and assessed through a Mutual Evaluation of the ESAAMLG. The report addresses any shortcomings in the area of AML/CFT and progress reports at regular intervals by the country.

k) The Financial Action Task Force (The "FATF")

The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions. The objectives of the FATF are to set standards and promote

effective implementation of legal, regulatory and operational measures for combating: money laundering, terrorist financing and other related threats to the integrity of the international financial system. The FATF is therefore a "policy-making body" which works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas.

The FATF has developed a series of recommendations that are recognized as the international standard for combating of money laundering and the financing of terrorism and proliferation of weapons of mass destruction. They form the basis for a coordinated response to these threats to the integrity of the financial system and help ensure a level playing field. First issued in 1990, the FATF Recommendations were revised in 1996, 2001, 2003 and 2012 to ensure that they remain up to date and relevant, and they are intended to be of universal application.

It should be noted that Mauritius follows all the FATF Recommendations as ESAAMLG is an FATF Associate Member and Mauritius is an ESAAMLG Member.

l) The United Nations Security Council (the "UNSC")

The United Nations Security Council has primary responsibility for the maintenance of international peace and security. It has 15 Members, and each Member has one vote. Under the Charter of the United Nations, all Member States are obligated to comply with Council decisions.

The Security Council takes the lead in determining the existence of a threat to the peace or act of aggression. It calls upon the parties to a dispute to settle it by peaceful means and recommends methods of adjustment or terms of settlement. In some cases, the Security Council can resort to imposing sanctions or even authorize the use of force to maintain or restore international peace and security.

The UNSC regularly issues resolutions to impose sanctions linked to individuals, entities, organizations, vessels and countries with which there is prohibitions to deal with and conduct any kind of business relationships. In this regard, the FIU send to every reporting person in our case, the Company, the resolutions whereby sanctions are passed or waived against individuals, entities, organizations, vessels and countries. These resolutions are saved on the database of the Company whereby every employee has access to verify any new business relations with the resolutions.

CHAPTER 3: OFFENCES: MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION OFFENCES

a) What is Money Laundering?

Money laundering (''ML'') is a generic term used to describe 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.

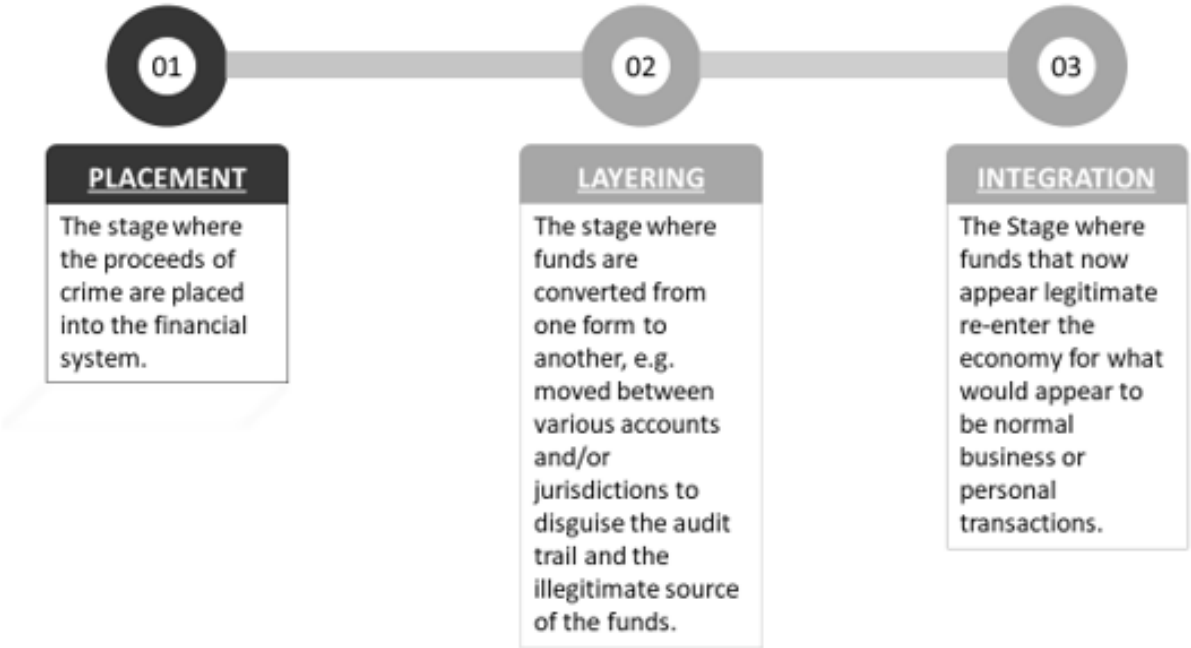
Illegal arms sales, smuggling, and the activities of organized crime, including for example, drug trafficking and prostitution, can generate huge profits. Embezzlement, insider trading, bribery and computer fraud schemes can also produce large profits and create the incentive to "legitimise" the ill-gotten gains through ML. When a criminal activity generates substantial profits, the individual or group involved must find a way to control the funds without attracting attention to the underlying activity or the persons involved. Criminals do this by disguising the sources, changing the form, or moving the funds or assets to a place where they are less likely to attract attention and disguising ownership and control

b) Money Laundering Mechanism

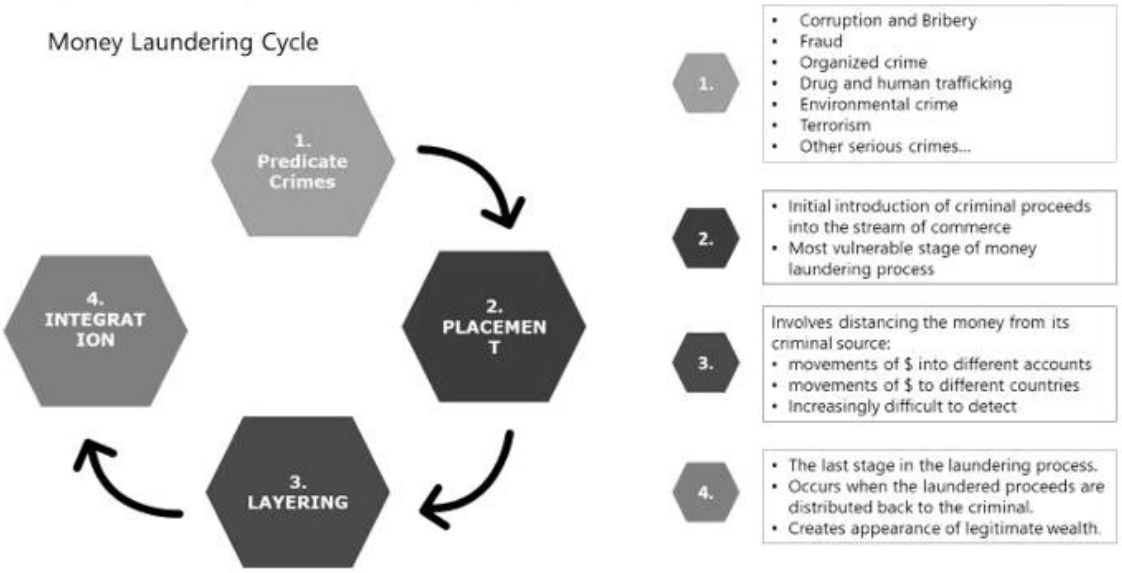
Money laundering has been described as a process that takes place in three stages as follows:

- Placement
- Layering; and
- Integration

Money Laundering Process



Money Laundering Mechanism



c) What is financing of Terrorism?

Terrorist financing is an activity that supports future illegal acts and both money laundering and terrorist financing require the assistance of the financial sector and skilled professionals such as accountants, bankers, investment manager and lawyers. The money used to finance terrorism can be derived from legitimate sources and the acts of terror usually occur at a future point in time after necessary financial services have been provided.

Terrorists often control funds from a variety of sources around the world which may be legitimately derived and employ increasingly sophisticated techniques to move these funds between jurisdictions. There may be a considerable overlap between the movement of terrorist funds and the laundering of criminal assets; terrorist groups often have links with other criminal activities.

There are, however, two major differences between the use of terrorist and other criminal funds: often only small amounts are required to commit a terrorist act and this makes terrorist funds harder to detect. Terrorism can be funded from legitimately obtained income such as donations and it will often not be clear at what stage legitimate earnings become terrorist assets.

The key to the prevention of both money laundering and terrorist financing is the adoption of adequate CDD measures both at the commencement of every relationship and on an on-going basis thereafter.

d) The consequences of money laundering and terrorist financing

Increased abuse of the financial system by criminal actors leads to increased criminal activity and less safety for everyone in the country and around the world. ML/TF can have serious negative consequences for the economy, national security and society in general. Some of these consequences may include:

a) Reputational damage from being perceived as being a haven for money launderers and terrorist financiers, leading to legitimate business taking their business elsewhere;

b) Attracting criminals including terrorists and their financiers to move to or establish new business relationships within the jurisdiction;

c) Damaging the legitimate private sector who may be unable to compete against front companies;

d) Weakening of financial institutions which may come to rely on the proceeds of crime for managing their assets, liabilities and operations, plus additional costs of investigations, seizures, fines, lawsuits etc.;

e) Economic distortion and instability; or

f) Increased social costs to deal with additional criminality such as policing costs or hospital costs for treating drug addicts.

CHAPTER 4: CORPORATE GOVERNANCE

At the Company, we abide by the following structure of lines of defense, with the first line being the client facing officers, the second line being the internal audit or compliance and risk management team and the third line being the audit and assurance testing through an Independent AML Audit of the frameworks in place for the Company. All lines of defenses report to the Board and are governed by the policies, controls and procedures of the Company.

First Line of Defense	- The Administrator's staff managing the Company - The Corporate Officers - The Finance Team
Second Line of Defense	- The Compliance Officer of the Company - The MLRO of the Company - The Compliance Team
Third Line of Defense	- The AML Independent Auditor

Each line of defense should jointly or severally ensure that they are the shield of the Company against any ML/TF or PF risk. This means that each line of defense has as their duty to ensure that they abide by all the Anti money laundering obligations stipulated herein this Manual through policies, procedures, and controls to be adhered to.

a) Responsibility of the Board of Directors for Compliance

The Board of Directors (the "Board") of the Company have through their governance, built an environment of trust, transparency, and accountability in the Company.

The Board moreover demonstrates its responsibility towards compliance in the following manner:

- evaluate all potential risks, including those of Money Laundering and Terrorist Financing;
- establish a formal strategy to counter money laundering and financing of terrorism;
- document its systems and controls (including policies and procedures); and
- clearly apportion responsibilities of the Compliance Officer and the MLRO for countering money laundering and financing of terrorism.

b) Responsibilities of Senior Management for Compliance

- To design, establish and maintain a compliance function and related policies and procedures, keeping in mind the prevalent regulatory practices of the region where the Company operates and the strategic moral and ethical obligations of the Company to its stakeholders.
- To designate a suitable person, who has the appropriate competence, to have the day to-day responsibilities for the Company's compliance with regulatory requirements.
- To identify and assess on an ongoing basis the new or changed compliance requirements applicable to the Company by any regulatory authorities; and take steps to modify existing policies and procedures to comply with the new or changed requirements.
- To provide compliance advice and support in relation to new business initiatives and ensure that a robust compliance infrastructure is implemented for any new initiatives that are undertaken.

c) The Compliance Officer ("CO")

The CO is responsible for the implementation and ongoing Compliance of the Company with internal programmes, controls and procedures in accordance with the requirement of the FIAMLA and FIAML Regulations 2018.

d) Responsibilities of the Compliance Officer:

- To ensure effective management of the Company's compliance function.
- To advise management, during the inception of new business processes, of the underlying integrity and compliance implications of these processes.

- To ensure corporate-wide communication of the compliance policy and its implementation.
- To act as a central repository of all information on rules, codes and business practices and ensure dissemination to all appropriate people in the organization.
- To establish detailed written compliance procedures that should be followed by all staff members.
- To ensure that the compliance policies and procedures are observed and breaches, if any, are remedied immediately and disciplinary actions, if required, are taken against the personnel responsible for the breach.
- To report to the Board on all compliance issues and assist the senior management to make an informed judgment on the effectiveness of the corporate-wide compliance policy.
- To report promptly to the Board or the management, of any material compliance failures (e.g., failures that may attract a significant risk of legal or regulatory sanctions, material financial loss, or loss to reputation).
- To ensure that all requests and instructions of regulators are complied with in a timely and accurate manner.
- To ensure that day to day compliance monitoring and administration are carried out to specified standards.
- To ensure that all registrations with FSC and other regulatory authorities are current and up to date.
- To work with the legal advisors and ensure that valid agreements with contracting parties or counterparties are put in place for new business initiatives.
- To update compliance Manuals and procedures.
- To arrange training and development of staff on regulatory responsibilities.
- To manage the handling of complaints.
- To present a year Compliance report to the Board.
- To present the compliance programme for the year to the Board.

e) Money Laundering Reporting Officer (“MLRO”)

The MLRO is the person who is nominated to ultimately receive internal disclosures of suspicious transactions whereby any member of staff has sufficient ground that the transaction involves money laundering or the financing of terrorism.

The Company ensures that the MLRO and his team have the privacy and confidentiality required. Hence, the MLRO and his team have a separate office whereby any member of staff can make a disclosure for a suspicious transaction.

f) Deputy Money Laundering Reporting Officer ("DMLRO")

The Deputy Money Laundering Reporting Officer of the Company is shall exercise the functions and office of MLRO in the MLRO's absence.

g) Administrator

The Administrator of the Company is Credentia International Management Ltd ("Credentia" or the "Administrator"), a private company limited by shares, duly incorporated under the laws of Mauritius on 11th April 2012.

The Company has outsourced to Credentia its AML/CFTP obligations.

The AML/CFTP obligations carried out by the Administrator are the following:

- Drafting of AML/CFT and Internal Control Procedure Manual of the Company;
- Updating the AML/CFT and Internal Control Procedure Manual of the Company;
- Establishing client and business risk assessment policies and profiling systems of the Company;
- Conducting due diligence exercise on all principals and parties involved with the Company;
- Registration of Company with the Financial Intelligence Unit for reporting of suspicious transactions;
- Carrying out internal AML/CFTP audit by way of file review;
- Record Keeping.

CHAPTER 5: RISK BASED APPROACH

a) Identification and Mitigation of Risks

The Company should maintain a dynamic approach to risk assessment. For this reason, the Company expects that the AML related risk assessments can be subject to regular changes in line with the recommendations of the FATF FSC or any other regulatory bodies as well as relevant AML laws and same shall be updated in the present Manual accordingly.

The following policies, procedures and controls have been put in place by Credentia in order to identify, assess, understand, mitigate, manage, review and monitor any risks associated to the business of the Company.

The Company shall keep a Risk Register for all its clients, third party the Company deals with and any service providers affiliated to the Company, whereby the risk rating of the party, the date the risk assessment was conducted and the date for the next risk assessment will be stated.

b) Risk Profiling System and rating system of the Company the Company assesses the ML/CF/PF risks associated to its Clients and Business. This is conducted through:

1. A Client Risk Assessment Sheet: The Company will assess the risk of its clients based on multiple factors detailed below and attribute a risk rating to the client, this rating will determine the frequency of assessment, review and monitoring the client needs.

2. A Business Risk Assessment: The Company will evaluate its own risk based on its activities and transactions and other key factors. A risk rating will also be attributed to the business which will determine the frequency of assessment to be done.

3. A Service Provider Risk Assessment Sheet: The Company will assess the service providers to whom they have outsources some functions, the factors have been detailed below and the rating will further determine the frequency of assessment and the retention of service from the service provider.

c) Client Risk Assessment (CRA)

The Client Risk Assessment Sheet ascribe a risk rating to every client that is on-boarded. 5 different criteria have been factored in whereby each criterion has been sub-divided into other criteria.

- Client
- Services and Transactions
- The Company Graphic Risk
- Delivery Channel and Business Practices
- Use of Technology

The Client criteria takes into consideration the following factors and attributes a rating to each:

- Nationality and Jurisdiction of the natural person or entity
- Country of Residence of the natural person or entity
- Country in which Client conducts business
- Due Diligence undertaken on the Client and whether records of the CDD documents have been kept
- Whether the Client is an inherently high-risk client, meaning whether the client is a PEP, PEP Affiliate, non-face to face or a non- profit organisation
- If the Client is a structure that makes it hard to determine who is the beneficial owner (company, trust, foundation, partnership or any other structure)
- Whether the Client is a nominee of the UBO

The Services and Transaction criteria takes int account the following parameters:

- The services being offered to the client.
- Whether the client undertakes high value transactions.
- Whether the transactions are conducted in large volume and complex ways.
- Whether the client engages in transactions that are consistent with ML/TFP red flags.

The Company graphic Risk criteria evaluated the Company graphic location of the funds with regards to sanctioned and high-risk countries and bases it assessment on the FATF list and the UN sanctions list.

The Delivery Channel and Business Practices criteria evaluated the way the transactions are being carried out and assesses the following:

- Whether cash payments and transactions have been accepted
- Whether transactions where the Company never met the client are affected
- Whether the source of funds of the client can be verified and justified
- Whether any payments have been made to unknown or unassociated third parties by the client
- Whether the client has been referred by a third party

Frequency of Customer Risk Assessment

The Customer Risk Assessment Exercise should be performed:

- Annually for higher risk customers or whenever a transaction with a high risk country or high risk customer occurs
- Every 2 years for medium risk customers subject to sector specific guidance;
- Every 3 years for Low-risk customers; and
- At the point of a material change in the customer's circumstances, for example establishing connections with a higher risk jurisdiction or engaging in a higher risk business.

d) Business Risk Assessment Sheet (BRA)

Business Risk Assessment will evaluate the risk related to the business of the Company and will take into account the following criteria:

- Services and transactions
- Clients' Risk
- The Company graphic Risk
- Delivery Channel and Business practices
- Use of technology

The services and transaction criteria will evaluate the following with regards to the services provided by the Company:

- the risk of the service offered to the Clients
- whether client of the Company undertake high value transactions
- whether the transactions of its clients are conducted in large volume and are complex by nature
- whether its clients engage in transaction consistent with red flags of ML and TFP

The Clients' Risk criteria evaluate the risks associated to the types of client that the Company has in its portfolio and the percentage for each, this includes:

- PEP clients
- Clients with a criminal record
- High risk clients
- Government owned entities
- Natural persons

The Company graphic Risk criteria evaluated the Company graphic location of the funds with regards to sanctioned and high-risk countries and bases it assessment on the FATF list and the UN sanctions list.

The Delivery Channel and Business Practices criteria evaluated the way the transactions are being carried out and assesses the following:

- Whether cash payments and transactions have been accepted
- Whether transactions where the Company never met the client are effected
- Whether the source of funds of the client can be verified and justified
- Whether any payments have been made to unknown or unassociated third parties by the client Whether the client has been referred by a third party

Frequency of Business Risk Assessment

The Company understands that the risk assessment exercise must be performed as soon as the Company commence business and therefore undertakes to review its business risk on an annual basis and in case of trigger events.

e) Service Provider Risk Assessment Sheet (SRA)

The service provider risk assessment sheet evaluates the service providers to whom the Company has outsourced some services. The risk profiling will take into consideration the profile of the service provider with notably it's the Company graphic location. The risk assessment will also evaluate the type of services provided and the results of the CDD and screening done on the service provider.

Service providers includes but is not limited to the Administrator of the Company, the auditor and advisors.

The criteria are as follows:

- Service Provider's Profile and the Company graphic Risk
- Services being outsourced

- Used of technology

The Service Provider's profile and the Company graphic Risk criteria evaluated the country location and jurisdiction of the service provider as well as the due diligence conducted on the service provider and whether same are on record.

- The service outsource criteria takes into account the following:
- the risk associated to the service provided by the service provider.
- whether the service provider is licensed and regulated.

CHAPTER 6: CUSTOMER DUE DILIGENCE

Customer Due Diligence ("**CDD**") is one of the most crucial limbs of AML/CFT. This principle has often been linked with the jargon "Know Your Customer or KYC". We believe that it is primordial not only to know but also understand our customers. CDD is often referred to as a vital tool for the Combatting of Money Laundering.

a. Customer Identification and Verification

Identification and verification refer to establishing and verifying a customer's identity. Verification refers to the verification of elements of the identification information, by using independent reliable sources, which may include material obtained from the customer such as a passport to verify the customer's name. It is essentially the concept of the Company satisfying itself that its customer is who they say they are.

The Company must, based on the relevant CDD information collected, make an analysis of the information provided and make such appropriate verification using external database or source, and consider whether it is appropriate to collect further CDD information. CDD information comprises both identification and verification information and customer relationship information.

Regulation 3(1) of the FIAML Regulations 2018 imposes an obligation on the Company to identify his customer whether permanent or occasional and verify the identity of his customer.

The objective of customer identification is to identify and obtain information on all applicants for business and the principals thereof. Applicants for business include any person, persons or entities corporate or unincorporated that seek to form a business relationship or to carry out a one-off transaction with the Company. A principal of an applicant for business is any person who is a beneficial owner of or has a beneficial interest in or has direct or indirect control of any relationship established with the Company.

Identification and verification of the identity of the customer and its principals is undertaken

independently by requesting for and retention of the following information and documents on the verification subjects such as the natural beneficial owner/shareholder, the principals of the applicants for business (in case of a trust- the settlor, trustees, beneficiaries, protectors and enforcers; in case of other type of entity- fund directors, controlling shareholders, account signatories, significant partners including Limited Partners, any person operating under a power of attorney):-

Note: Failure to identify and verify customers is an offence under the FIAMLA.

The Company must have in place clear, documented procedures governing the following situations:

(a) identification and verification of the identity of their applicants for business and existing customers on a risk-based approach (including identifying and verifying the identity of any connected individuals such as beneficial owners and controllers of the applicant);

(b) determination of whether an applicant for business is acting or intending to act for a third party and;

(c) where the Company is unable to determine whether the applicant is acting for a third party or not, make a suspicious activity report pursuant to section 14 of the FIAMLA to the Financial Intelligence Unit;

(d) These procedures must be brought to the knowledge of and be readily available to all relevant staff for the creation of an effective internal compliance culture and all staff will be aware of the reporting chain and procedures to follow;

(e) All relevant employees must receive ongoing training that is tailored to their role and responsibilities within the business as detailed in Chapter 14 of this Manual.

In addition, the Company is required to 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. If the Company determines that the applicant is acting for a third party, then it must keep a record setting out:

(a) the identity of the third party (and any beneficial owners or associated persons as required);
(b) the proofs of identity required under Regulation 3 of the FIAML Regulations 2018; and
(c) the relationship between the third party and the applicant for business.

The Company shall undertake effective CDD measures:

- when accepting a new customer or establishing a new business relationship, whereby the true identity of all customers and other persons with whom the Company conducts

transactions must be verified and the finding of which will be reported to the Board and approval sought therefrom;

- when carrying out banking/electronic transactions or making funds transfers to an unknown party;
- when there is a suspicion of money laundering or terrorist financing;
- on a yearly basis, based on the risk profile of a customer.

b. Timing of Verification of Identity

Before the establishment of a new client relationship and before providing any financial service, the Company should take all reasonable measures to complete all CDD measures for all applicants for business.

The CDD measures should normally be completed **before** the establishment of the client relationship.

Identification and verification Data for natural persons – Table 1

No.	Data to be collected	Permissible methods for verifying data
1.	Legal name (including any former names, aliases and any other names used).	• Current valid passport • Current valid national identity card • Current valid driving licence *(where the Financial institution is satisfied that the driving licensing authority carries out a check on the holder's identity before issuing the licence)* In each case, the document must incorporate photographic evidence of identity.
2.	Gender	
3.	Date of birth	
4.	Place of birth	
5.	Nationality	
6.	Current residential address PO Box addresses are not acceptable	• any of the identity sources listed above; a recent utility bill issued to the individual by name; • a recent bank or credit card statement; or • a recent reference or letter of introduction from: (i) a financial institution that is regulated in Mauritius; (ii) a regulated financial services business which is operating in an equivalent jurisdiction or a jurisdiction that complies with the FATF standards; or (iii) a branch or subsidiary of a group headquartered in a well-regulated
7.	Permanent residential address (if different from current residential address)	

		overseas country or territory which applies group standards to subsidiaries and branches worldwide, and tests the application of, and compliance with, such standards. **'recent' means within the last three months.**
8.	Any public position held and, where appropriate, nature of employment (including self-employment) and name of employer.	A letter or other written confirmation of the individual's status from the public body in question and or any enhanced CDD; a letter or other written confirmation of employment.
9.	Government issued personal identification number or other government issued unique identifier.	The relevant government document.
10.	Verify match to source of funds and profile of the client.	Declaration and evidence
11.	Financial details	Declaration via Application form
12.	Employment Information	Declaration via Application form
13.	Trading Information and Knowledge	Declaration via Application form

NOTE: ***Where a particular aspect of an individual's identity changes (such as change of name, nationality, or any other forms as approved), a financial institution must take reasonable measures to re-verify that particular aspect of identity of the individual using the same methods prescribed by the table above. In case of high-risk customers, further verification should take place using a newly issued replacement for the expired document.***

c. Legal Arrangements or Legal Persons

Regulations 5, 6 and 7 of the FIAML Regulations 2018 lays down specific requirements where an applicant is a legal person or a legal arrangement.

For customers that are legal persons, financial institutions should identify and verify the identity of beneficial owners by obtaining information on:

(a) the identity of all the natural persons who ultimately have a controlling ownership interest in the legal person;

(b) where there is doubt under subparagraph (a) as to whether the person with the controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interests, the identity of the natural person exercising effective control of the legal person; and

(c) where no natural person is identified under subparagraph (a) and (b), the identity of the natural person who holds the position of senior managing official[3].

Where the underlying shareholders are not natural persons, financial institutions must '**drill down**' to establish the identity of the natural persons ultimately owning or controlling the business. A legal person may have one or more methods of data verification as provided in the right column and the method of data verification will apply according to the legal status of the person to be identified.

Identification and verification date for legal person – Table 2

Person / arrangement to be identified	Data to be identified	Methods of data verification
Underlying principals who are individuals	As per the requirements for natural person. Where the individual persons are such by virtue of their status as members of the board of directors of a relevant legal person (or equivalent – for examples partners in a partnership[4], or council members in a foundation), financial institutions are required to identify and verify the identity of all such persons.	As per the requirements for natural person. Where the legal person with which the underlying person is associated is low or standard risk, then the method of verification for each required piece of data will normally suffice and can be one of the above methods. However, where the legal person is high risk, or where a high-risk rating would otherwise be attached to the individual principal, then the methods of verification will depend on the riskiness of the relationship and more than one method will be necessary.
Private Companies Partnerships Sociétés Foundations Other legal persons	1. Legal status of body; 2. Legal name of body; 3. Any trading names; 4. Nature of business; 5. Date and country of incorporation / registration; 6. Official identification number (for example, fund number); 7. Registered office address; 8. Mailing address (if different); 9. Principal place of business / operations (if different); 10. Any other data which the financial institution considers to be reasonably necessary for the purposes of establishing the true identity of the legal person.	• Certificate of incorporation (or other appropriate certificate of registration or licensing); • Memorandum and Articles of Association (or equivalent); • Fund registry search, including confirmation that the person is not in the process of being dissolved, struck off, wound up or terminated; • Latest audited financial statements or equivalent; • Annual report or equivalent; • Personal visit to principal place of business; • Partnership deed or equivalent; • Charter of Foundation; • Acte de société; Certificate of good standing from a relevant national body;

		• Reputable and satisfactory third party data, such as a business information service; • Any other source of information to verify that the document submitted is genuine.

[4]including the General Partner(s) and Limited Partners under a Limited Partnership

For customers that are legal arrangements, it is vital to identify and verify the identity of beneficial owners–

(a) for trusts, on the identity of the settlor, the trustee, the beneficiaries or class of beneficiaries, and where applicable, the protector or the enforcer, and any other natural person exercising ultimate effective control over the trust, including through a chain of control or ownership;

(b) for other types of legal arrangements, on the identity of the persons in equivalent or similar positions.

We must collect the identification data concerning a legal person listed in the left-hand column of the table below, and verify that data in accordance with the following:

(a) The data to be collected applies to low, standard and high-risk applicants for business. Potential methods of data verification are listed in the right-hand column of the table.

(b) The appropriate number of methods for verifying the data will vary depending on the status of the person to be identified and the risk rating:

(i) For low-risk legal persons, verification of each piece of the required data may take place using one of the methods identified.

(ii) For standard and high-risk legal persons, verification of each item of the required data must take place using at least two of such methods wherever practicable.

Identification and verification date for legal person: Trusts – Table 3

Person / arrangement to be identified	Data to be identified	Methods of data verification
Underlying principals who are legal persons	As per the requirements for legal persons above In circumstances where an applicant for business which is a legal arrangement acts or purports to act on behalf of a	As per the requirements for legal persons above

	legal person, then identification and verification must take place not just in respect of that legal person, but also in respect of that legal person's underlying principals in accordance with the preceding row of this table.	
Legal arrangement	1. Legal status of arrangement (including date of establishment); 2. Legal name of arrangement (if applicable); 3. Trading or other given name(s) of arrangement (if applicable); 4. Nature of business 5. Any official registration or identifying number (if applicable); 6. Registered office address (if applicable); 7. Mailing address (if different); 8. Principal place of business / operations (if different); 9. Any other data which the financial institution considers to be reasonably necessary for the purposes of establishing the true identity of the legal arrangement. 10. Financial Background. 11. Source of funds 12. Trading Experience 13. Regulation status	• Trust deed or equivalent instrument; • Official certificate of registration (if applicable); • Where the above proves insufficient, any other document or other source of information on which it is reasonable to place reliance in all the circumstances.

Ownership Structure

For customers that are legal persons or legal arrangements, it is important to: -

- Understand the ownership and control structure of the customer.
- Determine who ultimately owns or controls the customer.

Accordingly, a structure chart showing the ownership and control of the applicant for business shall be included in the Client Acceptance Checklist to be submitted to the Board.

Appropriate Certification

Documentary evidence of identity other than original documents shall be certified by:

- lawyer, notary, accountant holding a recognised professional qualification;
- a serving police or customs officer;
- a senior civil servant;
- a member of judiciary;
- employees of an embassy or consulate;
- director or secretary of a regulated financial services business in Mauritius or in an equivalent jurisdiction[5];
- commissioner of oaths;
- a senior officer of a recognised banking institution.

The Certifier should clearly state his:

- Name;
- Address;
- Position/capacity;
- Date of certification; and
- Contact details to aid tracing of the certifier.

However, where an employee of the Company meets the customer face to face and has access to original identity documentation, he or she may take copies of it and certify it personally as a true copy of the original.

Individuals acting on behalf of applicants for business and customers

There might be cases where applicants for business and customers (particularly those which are legal persons) will have one or more individuals authorised to act on their behalf in dealing with financial institutions – for example, persons authorised to instruct the financial institution to transfer funds on the customer's behalf. Such authority may derive from a number of possible sources: for example, a power of attorney, or an authorised signatory mandate form, or a trust instrument.

CHAPTER 7: HIGH RISK SITUATIONS

a) High-Risk Clients of the Company

The Compliance Officer will provide and will continuously update a list/ Register of Clients that the Company considers to be of 'high risk,' such that enhanced due diligence procedures are warranted compared to the routine Customer Due Diligence Procedures.

Following are the examples of Clients (not an exhaustive list – NOTE High Risk Clients will be determined with a risk-based approach as per the Client Risk Assessment) who pose a high money laundering risk:

1. A Politically Exposed Person;

2. Senior Foreign Political Figure;

3. any member of a Senior Foreign Political Figure's Immediate Family, and any Close Associate of a Senior Foreign Political Figure;

4. Any Client resident in, or organized or chartered under the laws of, a Non-Cooperative Jurisdiction; Note: Non-Cooperative Jurisdiction means any foreign country that has been designated as non-cooperative with international anti-money laundering principles or procedures by an intergovernmental group or organization, such as the Financial Action Task Force on Money Laundering ("FATF")

5. Any Client who gives the Compliance Officer any reason to believe that its funds originate from, or are routed through, an account maintained at an "offshore bank", or a bank organized or chartered under the laws of a Non-Cooperative Jurisdiction; and

6. Any Client who gives the Compliance Officer any reason to believe that the source of its funds may not be legitimate or may aid terrorist activities.

The Company shall apply enhanced due diligence measures for the following higher risks relationships:

b) Politically Exposed Persons (PEPs)

Government leaders or public sector officials, who have been entrusted with prominent public functions in foreign, domestic and international organisations including their family members and close associates are considered to be PEPS and might pose a greater than normal money laundering risk by virtue of their potential to acquire or abuse public funds and to channel the proceeds of corruption to foreign jurisdiction.

As part of EDD measures, the PEP Declaration Form should be duly filled by all Politically Exposed Persons who shall be connected to any entity either managed or administered by the Company, giving details of their Net Worth, Source of Wealth and Funds amongst others.

Different categories of PEP

Level/ Category	Definition and example
International	PEPs representing a multinational body (e.g., European Union)
National	PEPs holding a political position at the national level (e.g., Prime Minister)
State	PEPs holding a political position at the state level (e.g., Regional Council)
Local	PEPs holding a political position at the local level (e.g., City Mayor)

Register of PEPs

The Company keeps a register of PEP which highlights any PEP affiliated to the Company. If the Company does not currently have any stakeholders who are PEPs, the register will then be empty. However, should any person affiliated to the Company become a PEP or PEP affiliate by any means, the register will be updated accordingly.

c) Clients from jurisdiction with strategic deficiencies and sanctioned countries as listed by the FATF and the United Nations Security Council (‘’UNSC”)

Dealing with customers or receipt of funds from a particular jurisdiction that has been identified by the UNSC or FATF and FATF-styled regional bodies as “Non-co-operative/High Risk” in the fight against money laundering or jurisdictions which have been linked with terrorist financing.

Note: The FATF list of Jurisdiction with Strategic Deficiencies and the UNSC Resolutions are frequently verified by the Company. Notifications are received from FIU when there are changes & updates in the UNSC list. The client database is screened against the updated UNSC list.

As an automatic screening measures, the on-going screening option on world check is also enabled.

The UNSC Resolutions as received from the FIU is saved on the system and updated as a table for reference when on boarding clients or during ongoing monitoring.

The FATF list of jurisdictions with strategic deficiencies and sanctioned countries is verified and consulted by the Company whenever there is a new business relationship or transaction at http://www.fatf-gafi.org/countries/#high-risk .

Prior to onboarding and while conducting ongoing monitoring, the Company also verifies the status of jurisdictions it is dealing with through the following website: https://www.knowyourcountry.com

which gives an overview of the sanctions related to the country.

d) Negative Press Articles or sanctions by the regulated authorities

Negative press is the term given to any negative information, whether alleged or factual. This could be anything from an allegation of fraud by a disgruntled former customer to an article in a newspaper relating to a criminal investigation.

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

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

CHAPTER 8: ENHANCED DUE DILIGENCE

As per the Regulation 12 of the FIAML Regulations 2018, the Company has implemented internal controls and other procedures to combat money laundering and financing of terrorism, including Enhanced Due Diligence ("**EDD**") procedures with respect to high-risk persons, business relations and transactions and persons established in jurisdictions that do not have adequate systems in place to combat money laundering and financing of terrorism.

a) Measures of Enhanced Due Diligence

Enhanced due diligence procedures must be applied to the business relationships with applicants for business falling under the areas described in Chapter 7. Such EDD may take the form of the following checks, although it is not restricted by them and would depend on the specific circumstances at hand:

- Any further information required to understand the nature and purpose of the business relationship;
- Establishing the source of wealth of the customer or any beneficial owner and underlying principal;
- Particularly scrutinise the various transactions of the client by setting lower monitoring thresholds for transactions connected to such business relationships as well as establish the source of fund through the Source of Company Declaration Form to be duly filled by client or beneficial owner;
- Conducting further checks on the client from either the customer or from independent sources and AML screening through platforms such as World Check;
- Additionally, if required, hire service providers in the country where the individual or entity is based to conduct EDD.

b) Declaration of Source of Fund ("DSOF") Form

For all transactions or wire transfers that are classified as High Risk or suspicious and Board has been apprised, a DSOF Form should mandatorily be filled by the client or beneficial owner stating the details of the beneficiary, purpose of transfer, name of remitter and description of the source of fund amongst others in order to ensure that money has been transferred from a legitimate source.

c) Declaration of Source of Wealth Form ("DSOW") Form

Under the Financial Intelligence and Anti Money Laundering Act 2002 and the AML/CFT Handbook of the FSC, the Company is under an obligation to verify the origin of the funds that are being invested by the client/beneficial owner via the entities. As part of documentary evidence, the client might be required in some cases to fill the declaration of Source of Wealth Form.

CHAPTER 9: SCREENING

a) World Check Screening Policies and Procedures

World-Check is a database and screening tool used around the world to help to identify and manage financial, regulatory and reputational risk. World Check formed part of the Thomson Reuters Risk Management Solutions suite before being transferred to Refinitiv after a merger deal with The Blackstone Group in October 2018. World-Check provides trusted information to help businesses comply with regulations and identify potential financial crime.

b) Terrorism Financing and Proliferation Offences

Proliferation financing Red Flags to be alert of:

The following is a non-exhaustive list of indicators/ red flags of PF, which are relevant for customer and transaction monitoring:

i. The customer's transaction involves an individual or entity in a foreign country associated with proliferation and/or sanctions evasion concern;

ii. The customer or counterparty or its address is similar to one of the parties found on publicly available lists of persons who have been denied export licences, or has a history of export control contraventions;

iii. The customer's transactions involve possible shell companies (e.g. companies that do not appear to have real business activities and display other shell company indicators);

iv. The customer is vague and resistant to providing additional information when asked;

v. The customer has a sudden change in business activities;

vi. The customer is known or believed to have previous dealings with individuals or entities in countries subject to UNSC sanctions; or

vii. Sudden/frequent changes in directorship/authorised signatories which are not well explained or intended to conceal links with individuals associated with sanctioned countries/activities.

Screening for Terrorism Financing and Proliferation Offences

Screening of Designated persons under the United Nations Security Council Resolutions ("UNSC Resolutions") is done by the Company on an ongoing basis through World Check screening tool which screens against sanctions lists.

In the event that any match is found, the Company conducts an investigation of whether the match is actually related to any party to the Company.

The automated system of World Check is not the only way of screening on which the Company relies. It is possible to do a Manual mapping of the sanction list. The Company has ascribed the AML compliance duties to the Administrators, which includes screening against sanctions lists, for this reason, the Administrator receives the updates of the FIU on changes to the consolidated UN lists, which are then saved in their server and inputted into a table which sets out the date of the change, name of the individuals or entities, the country location and what is the type of change (entry, removal…). This table is accessible to all the officers of the Company.

c) Implementation of Targeted Sanctions

Targeted sanctions, including financial sanctions, arms embargo and travel ban, and other measures established by the United Nations Security Council under Chapter VII of the Charter of the United Nations has been implemented by the Government of Mauritius through The United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019.

Determining a true match can often prove challenging due to a range of variables including language, cultural nuances, spelling, abbreviations, and aliases. UN sanctions lists, NSSEC list, as do others, contain other identifying information to assist in the identification of a true match or false positive.

Clients must be screened against the Consolidated List and NSSEC list and evidence of the screening must be recorded. Clients can be screened manually against designated persons lists by using the publicly available lists, which can be downloaded from the UN, FIU or the NSSEC websites.

d) Reporting obligations and procedures for Sanctions Reports

If a true match is identified by the Administrators, they will have to report the case directly to the MLRO and subsequently, the MLRO must immediately submit a report to the **National Sanctions Secretariat**, and to the **Financial Intelligence Unit**.

In accordance with section 23(4) of the Act, any person who holds, controls or has in his custody or possession any funds or other assets of a listed party must, not later than 24 hours of any notice issued under section 18(1) of the Act, notify the National Sanctions Secretariat in writing of:

(a) details of such funds or assets;

(b) the name and address of the listed party;

(c) details of any attempted transaction involving the funds or other assets, including –

(i) the name and address of the sender of the funds or assets;

(ii) the name and address of the intended recipient of the funds or assets;

(iii) the purpose of the attempted transaction involving the funds or assets;

(iv) the origin of the funds or assets; and

(v) where the funds or other were intended to be sent.

Reports will be completed by the MLRO using the template which can be downloaded from the NSSec website: http://nssec.govmu.org,

Further to filling the report, the MLRO shall resolve not to deal **under any circumstance** with the entity or person identified as a positive match under the sanctions list, as provided under Sections 23 and 24 of the UN Sanctions Act 2019. The MLRO will further communicate to everyone at the Administrator's office that they should no longer deal with the entity or individual identified as a positive match under the sanctions list. The MLRO should be consulted before **anything** is done with relation the client who is a positive match. The MLRO will then wait for further guidance from NSSec.

e) Freezing of Assets

Following a report for a positive match, it is understood that one of the measures available to the NSSec will be the freezing of the assets of the individual or entity identified as a positive match under the sanctions list.

Asset freezing refers to the blocking of bank accounts and other financial assets of persons listed in any sanctions lists. As per UN guidelines, the purpose of the assets freeze is to deny listed individuals, groups, undertakings and entities the means to support terrorism. To achieve this, the UN seeks to ensure that no funds, financial assets or economic resources of any kind are made available to listed parties for so long as they remain subject to the sanctions measures. The assets freeze applies to all assets owned or controlled by listed individuals, groups, undertakings and entities. It also applies to the funds that derive from property that they own or control, directly or indirectly, or that are owned or controlled by persons acting on their behalf or at their direction.

CHAPTER 10: SIMPLIFIED DUE DILIGENCE

In general, the full range of CDD measures should be applied by the Company. However, simplified CDD measures can be implemented in cases where lower risks have been identified and this corresponds to the situations outlined in Regulation 11 of the FIAML Regulations 2018 and where

the CDD measures are commensurate with the lower risk factors or any guidance issued. The possibility of applying simplified CDD measures does not remove from the Company its responsibility to adopt CDD measures, it only allows for application of reduced measures. The ultimate decision rests with the Company and there may be instances, depending on the level of risk and all the known circumstances (a high-risk relationship e.g. PEP, will be dealt with more caution rather than the routine CDD measures), where it is inappropriate to adopt these simplified measures.

An example of simplified CDD measure could be not requiring CDD documentation for beneficial owner of publicly listed entities. The Company could obtain and retain documentary evidence of the existence of the public fund and of its listed status, together with a copy of its annual report to verify that the individuals who purport to act on behalf of such entity have the necessary authority to do so.

a) Instances for applying Simplified Due Diligence measures

The Company can apply simplified CDD measures where –

(a) Lower risks have been identified and the simplified CDD measures shall be commensurate with the lower risk factors;

(b) There is a low level of risk, the Company shall ensure that the low risk identified is consistent with the findings of the national risk assessment;

Where the Company decides to adopt the simplified measures in respect of a particular applicant, it must:

(a) document that decision in a manner which explains the factors which it took into account (including retaining any relevant supporting documentation) and its reasons for adopting the measures in question; and

(b) keep the relationship with the applicant (including the continued appropriateness of using the simplified measures) under review, and operate appropriate policies, procedures and controls for doing so.

CHAPTER 11: THIRD PARTY RELIANCE

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

In a third-party reliance scenario, the third party should be **regulated**, **supervised** and **monitored** and subject to CDD in line with section 17C of the FIAMLA and record keeping requirements pursuant to section 17F of the FIAMLA and Regulation 21 of the FIAML Regulations 2018 which

provides for third party reliance. When reliance is placed on a third party that is part of the same financial group, the financial institution must ensure that the group applies the measures as applicable to regulation 21(4) of the FIAML Regulations 2018.

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

An example of a third-party reliance arrangement is in the context of investment fund (fund), a third-party reliance arrangement between the fund or its administrator and a relevant third party that acts as a fund distributor for its underlying investors is very common.

In order to ensure that these arrangements meet the FSC's expectations, an investment fund and its administrator should ensure that:

- there is a signed agreement between the fund or its administrator and the relevant third party, in which the third-party consents to being relied upon for these purposes and undertakes to provide any CDD information obtained immediately upon onboarding.

- the signed agreement contains clear contractual terms in respect of the obligations of the third party to obtain and maintain the necessary CDD records and to provide the CDD documents upon request; is not acceptable. This is of particular relevance where reliance is placed on a third party based in a jurisdiction that is subject to secrecy laws or similar restrictive rules; and

- policies and procedures are in place which set out an approach with regard to the identification, assessment, selection and monitoring of third-party relationships, including the frequency of testing performed on such third parties to deliver the necessary CDD documents when requested.

Reliance may only be placed on third parties to carry out CDD measures in relation to the identification and verification of a customer's identity and the establishment of the purpose and intended nature of the business relationship. Third parties may not be relied upon to carry out the ongoing monitoring of dealings with a customer, including identifying the source of wealth or source of funds.

The FSC recommends that regular assurance testing is carried out in respect of the third-party arrangements, to ensure that the CDD documents can be retrieved without undue delay and that the documentation received is sufficient pursuant to section 17(2)(v) of the FIAMLA.

The Company should take steps to ensure that any existing third-party reliance arrangements comply with the applicable AML/CFT legislation in this regard.

The Administrator and Compliance Officer of the Company shall test the efficacity if the EIC during compliance reviews or internal audit. The timeframe of receiving requested CDD documents on investors is one of the parameters that will be tested among others.

An Independent AML auditor or the regulators can test the effectiveness of an EIC in place as well.

CHAPTER 12: MONITORING TRANSACTIONS AND ACTIVITY

The regular monitoring of a business relationship, including any transactions and other activity carried out as part of that relationship, is one of the most important aspects of effective ongoing CDD measures under Regulation 3(1)(e) of the FIAML Regulations 2018.

It is vital that the Company understands a customer's background and is aware of changes in the circumstances of the customer and beneficial owner throughout the life cycle of a business relationship.

The Company can usually only determine when it might have reasonable grounds for knowing or suspecting that ML and/or TF is occurring if it has the means of assessing when a transaction or activity falls outside the normal expectations for a particular business relationship.

There are two strands to effective ongoing monitoring:

(a) The first relates to the transactions and activity which occur on a day-to-day basis within a business relationship and which need to be monitored to ensure they remain consistent with the financial institution's understanding of the customer and the product or service it is providing to the customer.

(b) The second relates to the customer themselves and the requirement for the financial institution to ensure that it continues to have a good understanding of its customers and their beneficial owners. This is achieved through maintaining relevant and appropriate CDD and applying appropriate ongoing screening.

a) Obligations

Under **Regulation 3(1) (d) of the FIAML Regulations 2018**, the Company should understand and obtain adequate and relevant information on the purpose and intended nature of a business relationship or occasional transaction. Further, in accordance with **Regulation 3(1) (e) of the FIAML Regulations 2018**, the Company should conduct ongoing monitoring of a business relationship, including –

(i) scrutiny of transactions undertaken throughout the course of the relationship, including, where necessary, the source of funds, to ensure that the transactions are consistent with his knowledge of the customer and the business and risk profile of the customer;

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

Regulation 12(2)(f) of the FIAML Regulations 2018 states that EDD measures that may be applied

for higher risk business relationships including conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

Regulation 15(1)(d) of the FIAML Regulations 2018 requires the Company to conduct enhanced ongoing monitoring on foreign PEPs, whether as customer or beneficial owner, in addition to performing the CDD measures. The same requirement applies in cases when there is higher risk business relationship with a domestic PEP or an international organisation PEP. Examples of the additional monitoring arrangements for high-risk relationships could include:

(a) undertaking more frequent reviews of high-risk relationships and updating CDD information on a more regular basis;

(b) undertaking more regular reviews of transactions and activity against the profile and expected activity of the business relationship;

(c) applying lower monetary thresholds for the monitoring of transactions and activity;

(d) reviews being conducted by persons not directly involved in managing the relationship, for example, the CO;

(e) ensuring that the Company has adequate MI systems to provide the board and CO with the timely information needed to identify, analyse and effectively monitor high risk relationships and accounts;

(f) appropriate approval procedures for high value transactions in respect of high-risk relationships; and/or

(g) a greater understanding of the personal circumstances of high-risk relationships, including an awareness of sources of third-party information.

The Company should also consider the possibility for legal persons and legal arrangements to be used as vehicles for ML and TF.

b) PEP Relationships

The system of monitoring used by the Company must provide for the ability to identify where a customer or beneficial owner becomes a PEP during the course of the business relationship and whether that person is a foreign PEP, domestic PEP or international organisation PEP.

In accordance with **Regulation 15(1) (b) of FIAML Regulations 2018**, where a customer or beneficial owner becomes a foreign PEP during the course of an existing business relationship, as part of the EDD measures subsequently applied the Company shall obtain senior management approval to continue that relationship. The same requirement applies in cases when there is higher risk business relationship with a domestic PEP or an international organisation PEP.

It is not expected that the Company will have a thorough knowledge of, or fully research, a family connection. The extent to which a connection is researched should be based upon the size, scale,

complexity and involvement of the person in the context of the business relationship and the profile of the business relationship, including its asset value.

It is possible that family members and/or associates may not inform the Company, or even be aware, of their PEP status and therefore independent screening and monitoring should be conducted. It is also possible that an individual's PEP status may not be present at take-on, for example, where that person takes office during the life of a business relationship. It is therefore important that ongoing monitoring exists in order to identify changes of status and risk classification.

c) High Risk Transactions or Activity

When conducting ongoing monitoring, the following are examples of red flags which may indicate high risk transactions or activity within a business relationship:

(i) an unusual transaction in the context of the Company's understanding of the business relationship (for example, abnormal size or frequency for that customer or peer group, or a transaction or activity involving an unknown third party);

(ii) funds originating from, or destined for, an unusual location, whether specific to an individual business relationship, or for a generic customer or product type;

(iii) transactions or activity unexpectedly occurring after a period of dormancy;

(iv) unusual patterns of transactions or activity which have no apparent economic or lawful purpose;

(v) an instruction to effect payments for advisory or consulting activities with no apparent connection to the known activities of the customer or their business;

(vi) the involvement of charitable or political donations or sponsorship; or

(vii) a relevant connection with a country or territory that has significant levels of corruption; or

(viii) provides funding or support for terrorist activities.

The Company must remain conscious that under the FIAMLA, they have an obligation to prevent and detect ML and TF.

A customer who is, or may be, attempting to launder money may frequently structure his instructions in such a way that the economic or lawful purpose of the instruction is not apparent or is absent entirely. When asked to explain circumstances or transactions, the customer may be evasive or may give explanations which do not stand up to reasonable scrutiny.

Where the Company is suspicious, or has knowledge of, money laundering or terrorist financing, it should not unquestioningly carry out instructions as issued by the customer.

If the Company unquestioningly carries out unreasonable instructions in this manner, it may mean that it is failing in its duty to prevent and detect ML/TF.

When faced with unreasonable customer instructions that lead the relevant person to know or suspect ML/TF, the Company must file a suspicious transaction report and consider taking legal advice.

d) Real-Time and Post-Event Transaction Monitoring

Transaction Monitoring procedures should involve a combination of real-time that is pre-transaction and post- transaction t monitoring.

Real-time monitoring focuses on transactions and activity where information or instructions are received before or as the instruction is processed whilst post-event monitoring involves periodic, for example monthly, reviews of transactions and activity which have occurred over the preceding period.

Real-time monitoring of activity can be effective at reducing exposure to Money Laundering, Terrorism Financing and Proliferation Financing offences whereas post-event monitoring may be more effective at identifying patterns of unusual transactions or activities.

In this respect, regardless of the split of real-time and post-event monitoring, the over-arching purpose of the monitoring process employed should be to ensure that unusual transactions and activity are identified and flagged for further examination.

The Company has established a layer of safeguards for both real time transaction monitoring as well as post transaction monitoring and ensures that red flags/alerts raised are examined within the shortest delay and properly documented.

1. Real Time Monitoring of Transaction Procedure at Credentia

Outgoing Funds Monitoring

Outgoing transactions are monitored on Real Time by Credentia. Upon receipt of a transfer instruction from client, the administrators focus on understanding the rationale of the transaction, verifying whether the transaction is in line with the business activity of the firm and gathering all supporting documents related to the transaction. Once all documents are gathered the Wire Request Checklist is filled and subsequently approved by the team manager.

2. Post Transaction Monitoring Procedure at Credentia

Incoming Funds Monitoring

A bank analysis exercised is performed to understand the rational of the funds which have been received by the firm on a weekly basis. Administrators also collect all relevant supporting documents to understand the purpose the funds are being transferred in and assess whether the transaction is in line with the activity of the firm. The bank analysis is prepared using excel templates which are shared for review.

The transactions are also monitored by the Compliance Officer at the Company when he performs

his Compliance Review. He ascertains that the supporting documents are available in file and are in order.

The Company screens the transactions against the Consolidated List and NSSEC list. Each incoming and outgoing transaction should be screened for a potential match with sanctions lists. Screening should be focused at a point in the transaction where detection of sanctions risk is actionable – where a transaction can be stopped and funds frozen if required – and before a potential violation occurs

Insight into bank accounts is given to the Administrator/ Management Company via 'online viewing rights'

For proper transaction monitoring, it is essential that the Administrator/ Management Company has (preferably digital access) to all bank accounts of the Company, whether it authorises payments to the bank accounts or not.

Transactions can be reviewed prior to implementation (real-time monitoring) or afterwards, when the transaction has already been executed (post-event monitoring).

The CO of the Company or the Administrator in its internal audit of the Company can do samplings of the transactions and review them.

An Independent AML auditor can sample the transactions for testing purposes as well.

The frequency on which the statements are obtained and monitored, should be appropriate for the risk profile of the Company.

Adequate documentation of all-monitoring and related transactions activities

The record of transactions monitored should be able to demonstrate the following:

- which transactions are selected and the reasons for selecting them?
- what aspects of the transactions and supporting documents have been reviewed?
- whether the Compliance officer has been involved, and
- what decision was ultimately made and on what grounds?

At every stage, roles, responsibilities and authority levels that are assigned, with every decision or remark recorded.

Reassessment of previous and related transactions if a suspicious transaction is identified

In the event that an unusual transaction is flagged up, the MLRO shall go back and review previous and related transactions. Such a review could provide insight into possible unusual transaction patterns and allow the risk and transaction profile of the client to be reviewed before further activity can resume.

e) Periodic Testing of Transaction Monitoring Process

As part of its internal AML audit of the Company and as part of its periodically test the effectiveness of their transaction monitoring process with a view to carrying out trend analyses, so full access to past data is crucial.

3. Call Back for clients

The Company also has in place an internal system of call back procedures for its clients.

The call back will apply for any transaction that is requested (reimbursement of funds, payment of invoices…), the procedures will further apply to all amount regardless of whether it is small or large.

The designated officers on receiving of an instruction to transfer funds to the client will call the client to verify if he has requested for a transfer to be made.
Once it is confirmed that it was the client that requested for the payment to be made, the officer will go through the internal process to enable the transfer to be done.

4. Examination

In accordance with **Regulation 25(1) of FIAML Regulations 2018**, where within a business relationship there are complex, or large and unusual transactions, or unusual patterns of transactions, which have no apparent economic or lawful purpose, the Company shall examine the background and purpose of those transactions.

As part of its examination, the Company should give consideration to the following:

(a) reviewing the identified transaction or activity and the CDD information held;

(b) understanding the background of the activity and making further enquiries to obtain any additional information required to enable a determination to be made by the Company as to whether the transaction or activity has a rational explanation and economic purpose;

(c) reviewing the appropriateness of the relationship risk assessment in light of the unusual transaction or activity, together with any supplemental CDD information obtained; and

(d) considering the transaction or activity in the context of any other connected business relationships and the cumulative effect this may have on the risk attributed to those relationships.

For the purposes of **Regulation 25(1) of FIAML Regulations 2018**, what constitutes a large and unusual or complex transaction will be based on the particular circumstances of a business relationship and will therefore vary from customer to customer.

The Company must ensure that the examination of any large and unusual, complex, or otherwise higher risk transaction or pattern of transactions or other activity is sufficiently documented and that such documentation is retained in a readily accessible manner in order to assist the FSC, the FIU,

other domestic competent authorities and auditors.

The Company must ensure that procedures are maintained which require reporting of internal disclosures to be made to the MLRO in accordance with the requirements of **Regulations 27 (c) of FIAML Regulations 2018** and Chapter 14 of this Manual where any information or other matters that come to the attention of the file handler and his opinion gives rise to any knowledge or suspicion that another person is engaged in money laundering and terrorism financing activity.

Following the conclusion of its examination, the Company should consider whether follow-up action is necessary in light of the identified transaction or activity. This could include, but is not limited to:

(a) applying EDD measures where this is considered necessary or where the financial institution has reassessed the business relationship as being high risk as a consequence of the transaction or activity;

(b) considering whether further employee training in the identification of large and unusual, complex, or higher risk transactions and activity is needed;

(c) considering whether there is a need to adjust the monitoring system (for example, refining monitoring parameters or enhancing controls for more vulnerable products, services and/or business units); and/or

(d) applying increased levels of on-going monitoring for particular relationships.

f) Ongoing CDD

In accordance with **Regulation 3(1) (e)(ii)**, the requirement to conduct ongoing CDD will ensure that the Company is aware of any changes in the development of a business relationship. The extent of the Company's ongoing CDD measures must be determined on a risk-sensitive basis. However, the Company must be aware that as a business relationship develops, the risks of ML and TF may change.

It should be noted that it is not necessary to re-verify or obtain current identification data unless an assessment has been made that the identification data held is not adequate for the assessed risk of the business relationship or there are doubts about the veracity of the information already held. Examples of such could include a material change in the way that the business of the customer is conducted which is inconsistent with its existing business profile, or where the Company becomes aware of changes to a customer's or beneficial owner's circumstances, such as a change of address.

To reduce the burden on customers and other key principals in low-risk relationships, trigger events may present a convenient opportunity to review the CDD information held.

The review must take account of the CDD and EDD obtained on the customer, whether there have been any changes to the customer's activity / circumstances. Where the basis of a relationship has changed the relevant person should consider whether the risk rating of the customer needs amending and carry out further CDD procedures to ensure that the revised risk rating and basis of the relationship is fully understood. Ongoing monitoring procedures must take account of these changes.

If the risk changes significantly it should be remembered that EDD may be required. The review should include considering the customer's location in relation to the high risk third countries and sanctions list.

The Company must ensure that any updated CDD information obtained through meetings, discussions, or other methods of communication with the customer is recorded and retained with the customer's records. That information must be available to the MLRO.

Failure to adequately monitor customers' activities could expose a business to potential abuse by criminals and may call into question the adequacy of systems and controls, or the prudence and integrity or fitness and properness of the management of the business.

g) Oversight of Monitoring Process by Compliance Officer

The CO should have access to, and familiarise herself with, the results and output from the Company's monitoring processes. Such output should be reviewed by the CO who in turn should report regularly to the board, providing relevant management information such as statistics and key performance indicators, together with details of any trends and actions taken where concerns or discrepancies have been identified.

The board should consider the appropriateness and effectiveness of the Company's monitoring processes as part of its annual review of the Company's associated policies, procedures and controls.

This should include consideration of the extent and frequency of such monitoring, based on materiality and risk.

Where the Company identifies weaknesses within its monitoring arrangements, it should ensure that these are rectified in a timely manner.

CHAPTER 13: SUSPICIOUS TRANSACTION REPORTING

a) Suspicious Transaction

A suspicious transaction remains one for which there are reasonable grounds to suspect that the transaction is related to a money laundering offence, or you have reasonable grounds to suspect that the transaction is related to financing a terrorist activity.

The MLRO of the Company shall forthwith make a report to the Financial Intelligence Unit ('FIU') of any transaction which the Company has reason to believe may be a suspicious transaction.

b) Identification of Suspicious Transaction

The Money Laundering Reporting Officer (MLRO) of the Company shall have to assess whether there are reasonable grounds to suspect that a transaction is related to money laundering offence or a terrorist activity financing offence.

c) Making a Suspicious Transaction Report

Once you have detected a fact that leads you to have reasonable grounds to suspect that a transaction is related to money laundering, proceeds of any crime or financing of activities related to terrorism, a suspicious transaction report form (STR) must be sent to FIU within 5 days by the MLRO.

It is the information about the transaction and about what led to suspicion that is important in a STR.

The report should provide maximum details on what led to suspicion including anything that made the MLRO suspect that it might be related to money laundering, terrorist financing, or both. If distinction cannot be made based on the information available, remember that it is the information about 'suspicion' that is important, not the distinction between money laundering and terrorist activity offences.

Photostat copies of document facilitating the identification of the party or parties to the transaction should be enclosed with the STR. Other forms of evidence can be Identity Card number, Birth Certificates, Passport and References from banks. Also enclose handwriting sample and a photograph of the suspected party or parties, if available.

d) Lodging of Reports of Suspicious Transactions

Every report under section 14 shall be lodged with the FIU.

For the purposes of this Part, every report shall be in such form as the FIU may approve and shall include –

1. the identification of the party or parties to the transaction;

2. the amount of the transaction, the description of the nature of the transaction and all the circumstances giving rise to the suspicion;

3. the business relationship of the suspect to the Company;

4. where the suspect is an insider, any information as to whether the suspect is still affiliated with the Company;

5. any voluntary statement as to the origin, source or destination of the proceeds;

6. the impact of the suspicious activity on the financial soundness of the reporting institution or person; and

7. the names of all the officers, employees or agents dealing with the transaction.

e) Recording Suspicious Transaction Reports

A register of Internal Disclosure Reports received by the MLRO and all reports made by the MLRO to the FIU will be maintained. Where the MLRO has not deemed it appropriate to report a transaction

reported by an employee he or she should document the reasons (for not submitting it) on the register. The FSC will routinely inspect suspicious transaction report registers during the course of compliance visits.

f) Offence of Tipping Off

Section 19(1)(c) of the Financial Intelligence and Anti Money Laundering Act 2002 provides for the offence of "tipping off" which offence is committed when a person, knowingly or without reasonable excuse, warns or informs the owner of any funds of any report or any action that is to be taken in respect of any transaction concerning such funds.

When a suspicious transaction report has been made to the FIU with respect to a particular customer, the officer must ensure that due care is taken during subsequent enquiries so as not to alert the client about the disclosure.

Moreover, as a reporting person, the MLRO of the Company is not allowed to inform anyone, including the client, about the contents of a suspicious transaction. As it is important not to tip such client off that the MLRO is making a suspicious transaction report, it is important that no further information or document is requested from the client that would normally not request during a normal transaction.

g) Records of Suspicious Transaction Reports

The Company is mandated to maintain records of Internal Disclosure Reports and suspicious transaction reports made to the FIU. 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.

h) Immunity

No criminal or civil proceedings may be brought against the Company and its officers for making a report in good faith concerning a suspicious transaction. This also applies if the Company is not required to submit a report to FIU but decide to provide information voluntarily to FIU because of suspicions of money laundering or financing of terrorist activity.

i) Penalties

There are penalties if the Company fails to meet the suspicious transaction reporting obligations. Failure to report a suspicious transaction could lead to up to five years' imprisonment and a fine of not exceeding Rs 1,000,000.

CHAPTER 14: RECORD KEEPING

a) Records obtained through CDD measures:

All records obtained through CDD measures, including account files, business correspondence and copies of all documents evidencing the identity of customers and beneficial owners, and records and the results of any analysis/assessment undertaken in accordance with the FIAMLA, all of which shall be maintained for a period of not less than 7 years after the business relationship has ended.

b) Records of suspicious transaction reports

The Company is obliged to maintain records of Internal Disclosure Reports and suspicious transaction reports made to the FIU as well as registers of both internal suspicious transaction records as well as STRs submitted to the FIU. 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. These records are kept by the MLRO of the Company in locked cupboards and in restricted access files on the server to which only the MLRO and DMLRO have access.

c) Identity records and Transactional records

In order to assist law enforcement agencies to follow audit trails should the need arise, the Company shall maintain all documentation used to verify the identity of all applicants for business and records of all transactions undertaken during the course of a client relationship either in the form of original documents or copies of original documents (as required by the standard licensing conditions).

All identification and transactional records should be retained for a period of at least 7 years after the termination of the relationship or the completion of the transaction to which they relate, as the case may be.

Records shall include account records of the customer during the course of the relationship and shall be kept as long as prescribed under the relevant legislation and will also include any audit report of the different functions of the Company.

The following information should be kept for every transaction carried out in the course of a business relationship or one-off transaction:

(a) the name and address of the customer;

(b) if a monetary transaction, the kind of currency and the amount;

(c) if the transaction involves a customer's account, the number, name or other identifier for the account;

(d) the date of the transaction;

(e) details of the counterparty, including account details;

(f) the nature of the transaction; and

(g) details of the transaction.

d) Record keeping of training materials, attendance sheets and registers

The Company keeps record of all training provided to the employees. Copy of training materials of both internal and external trainings attended are kept on file as well as on server to enable staff to refer to such materials.

Records of attendance sheets of internal trainings are kept at the Legal and Compliance department of the Company together with training registers.

As for external trainings attended, the records including certificate of attendance are kept with the accounting department also responsible for HR.

e) Failure to keep records

In the event the Company destroys or removes any record (which includes register or document as per section 17F of the FIAMLA); or fails to warn or inform the owner of any funds of any report required to be made in respect of any transaction or any action to be taken with respect to any transaction; or facilitates or permit a transaction to be carried out under a false identity commits an offence and on conviction is liable to a fine not **exceeding one million rupees and to imprisonment for a term not exceeding 5 years.**

CHAPTER 15: COMPLIANCE CULTURE, TRAINING AND EMPLOYEE SCREENING

a) Establishing a culture of compliance at the Company

The Company aims at establishing a culture of compliance that embeds compliance into everyday workflow and sets the foundation and expectations for individual behaviour across the Company through regular trainings, knowledge sharing and discussions on AML/CFT at different levels in the Company.

b) Trainings

One of the most important tools available to financial institutions, to assist in the prevention and detection of financial crime, is to have appropriately screened employees who are alert to the potential risks of ML and TF and who are well trained with respect to the CDD requirements and the identification of unusual activity, which may prove to be suspicious.

The effective application of even the best designed systems, policies, procedures and controls can be quickly compromised if employees lack competence or probity, are unaware of, or fail to apply, the appropriate policies, procedures and controls or are not adequately trained.

The Company is required, under Regulation 22(1)(b) of FIAML Regulations 2018, to implement programmes for screening procedures so that high standards are maintained when hiring employees. Furthermore, Regulation 22(1)(c) of FIAML Regulations 2018 states that programmes against money laundering and terrorism financing should also be in place to include ongoing training

programme for the directors, officers and employees of the financial institution, to maintain awareness of the laws and regulations relating to money laundering and terrorism financing to:

(i) assist them in recognising transactions and actions that may be linked to money laundering or terrorism financing; and

(ii) instruct them in the procedures to be followed where any links have been identified under sub subparagraph (i).

c) Annual AML/CFT Training

All employees are provided with training on anti-money laundering measures and in the recognition and handling of suspicious transactions as per AML/CFT legislations including this Manual. In-house AML/CFT trainings are provided at least once a year to all the staff of the Company by the MLRO, Compliance Officer or any other qualified trainer.

d) Ongoing Professional Development Training

The Company ensures the MLRO and DMLRO are provided with ongoing professional development trainings including participating in professional associations and conferences. In addition, MLROs and DMLRO should receive in depth training on all aspects of the prevention and detection of ML/TF.

Additionally, the Company makes it a must that the Compliance Officer receives in depth training on all aspects of the prevention and detection of ML/TF, including, but not limited to, addressing the monitoring and testing of compliance systems and in place to prevent and detect ML and TF.

Moreover, the Board of directors and senior management are required to follow advance trainings on anti-money laundering measures, in view of their particular responsibilities and appropriate to their roles.

e) AML/CFT Training for New Staff

Within 14 days of being employed but in any event before a new employee begins to engage in the provision of financial services, he/she must receive anti money laundering awareness training and training on the anti-money laundering procedures that are in place within the Company. Trainings are usually followed by an assessment to evaluate the level of understanding of the staff on the subject matter and whether further in-depth guidance is required. However, it should be noted that any such employee, if employed in a junior position, is not in direct touch with the client and any e-mails that are sent to the client are always monitored first-hand by the manager in charge.

The employees are also usually notified that due to the nature of the business of the Company, they should maintain a high level of awareness and vigilance whilst discharging their responsibilities at all times.

f) Employee Screening

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

a. obtaining and confirming details of employment history, qualifications and professional memberships;

b. obtaining and confirming appropriate references;

c. obtaining and confirming details of any regulatory action or action by a professional body taken against the prospective employee;

d. obtaining and confirming details of any criminal convictions, including the provision of a check of the prospective employee's criminal record; and

e. screening the employees against the UN's list of designated persons under terrorist and proliferation financing targeted financial sanctions.

will to carry out periodic ongoing screening of its employees against the UN's list of designated persons under terrorist and proliferation financing targeted financial sanctions. This task is carried out both through automatic screening as well as Manual verification of the UNSCR Sanctions lists.