# ANTI MONEY LAUNDERING

# COUNTER TERRORISM FINANCING

# &

# PROLIFERATION OF WEAPONS OF MASS DESTRUCTION

# MANUAL

GMBB Investment Ltd

**April 2023**

| | |
|---|---|
| Document Title | AML CFT Manual |
| Authorship | Risk and Compliance Team |
| Draft Circulated on | 20 April 2023 |
| FV approved on: | 5 May 2023 |
| Approved by | Board of Directors |

## Table of Contents

1. DEFINITIONS ..... 1

2. INTRODUCTION ..... 4

3. BOARD OF DIRECTORS RESPONSIBILITY FOR COMPLIANCE ..... 5

4. COMPLIANCE FUNCTION ..... 6

5. GENERAL PRINCIPLES FOR MARKET PRACTISE AND CODE OF CONDUCT ..... 12

6. DESCRIPTION OF MONEY LAUNDERING,TERRORIST AND PROLIFERATION FINANCING ..... 13

7. AML/CFT INTERNAL CONTROLS, POLICIES AND PROCEDURES ..... 16

8 RECORD KEEPING ..... 60

9 EMPLOYEES' SCREENING, EDUCATION AND TRAINING ..... 63

10 REPORTING TO THE FIU ..... 68

11 INDEPENDENT AUDIT ..... 72

ANNEX I ..... 76

ANNEX II ..... 82

ANNEX III ..... 83

ANNEX IV ..... 85

ANNEX V ..... 87

ANNEX VII ..... 88

ANNEX VIII ..... 89

ANNEX IX ..... 91

## 1. DEFINITIONS

a) **Act means** the Financial Intelligence and Anti-Money Laundering Act 2002 (FIAMLA) (as amended);

b) **Act of terrorism** means an act which:

(a) may seriously damage a country or an international organisation; and

(b) is intended or can reasonably be regarded as having been intended to-

(i) seriously intimidate a population;

(ii) unduly compel a Government or an international organisation to perform or abstain from performing any act;

(iii) seriously destabilise or destroy the fundamental political, constitutional, economic or social structures of a country or an international organisation; or

(iv) otherwise influence such government, or international organisation; and;

c) **AML** means Anti-Money Laundering;

d) **AML/CFT** means anti-money laundering and combatting the financing of terrorism and proliferation;

e) **Applicant for business** means a person, who seeks to form a business relationship, or carry out a one-off transaction with a relevant person;

f) **Beneficial Owner** means:

a. means the natural person:
    i. who ultimately owns or controls a customer; or
    ii. on whose behalf a transaction is being conducted; and
b. includes those natural persons who exercise ultimate control over a legal person or arrangement and such other persons included in the Act and Regulations

g) **Business relationship** means an arrangement between a person and a relevant person, where the purpose or effect of the arrangement is to facilitate the carrying out of transactions between the person and the relevant person on a frequent, habitual or regular basis;

h) **CFT** means Counter Financing of Terrorism;

i) **Customer**, in relation to a transaction or an account, includes:

i. the person in whose name a transaction or account is arranged, opened or undertaken;

ii. a signatory to a transaction or account; or

iii. any person to whom a relationship or an account or rights or obligations under a transaction or relationship have been assigned or transferred; or any person who is authorised to conduct the transaction or control the relationship or account; or

iv. such other persons prescribed for the purposed of this definition;

j) **Company** means GMBB Investment Ltd which is a private limited company incorporated in Mauritius with Company registration number 195321GBC and GB22201139

k) **Money Laundering Reporting Officer (MLRO)** means an officer appointed pursuant to the Regulation referring to Money Laundering

l) **Money Laundering (ML)** means

1. any person who:

(a) Engages in a transaction that involves property which is, or in whole or in part directly or indirectly represents, the proceeds of any crime; or

(b) receives, is in possession of, conceals, disguises, transfers, converts, disposes of, removes from or brings into Mauritius any property which is, or in whole or in part directly or indirectly represents, the proceeds of any crime,

where he suspects or has reasonable grounds for suspecting that the property is derived or realized, in whole or in part, directly or indirectly from any crime, shall commit an offence.

2. A bank, financial institution, cash dealer or member of a relevant profession or occupation that fails to take such measures as are reasonably necessary to ensure that neither it nor any service offered by it, is capable of being used by a person to commit or to facilitate the commission of a money laundering offence or the financing of terrorism shall commit an offence.

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

m) **National Committee** means the National Committee for Anti- Money Laundering and Combating the Financing of Terrorism and Proliferation.

n) **Person** includes a body of persons whether it has legal personality or not means any natural or legal person and includes any statutory body, company or association or body of persons corporate or unincorporated;

o) **Regulations** means the regulations made under this Act i.e. the Financial Intelligence and Anti-Money Laundering Regulations of 2018 as amended;

p) **Suspicious transaction** means a transaction which:

a) Gives rise to a reasonable suspicious that it may involve –

(i) the laundering of money or the proceeds of any crime; or

(ii) funds linked or related to, or to be used for, terrorist financing or by proscribed organisations, whether or not the funds represent the proceeds of a crime;

b) is made in circumstances of unusual or unjustified complexity;

c) appears to have no economic justification or lawful objective;

d) is made by or on behalf of a person whose identity has not been established to the satisfaction of the person with whom the transaction is made; or

e) gives rise to suspicion for any other reason.

q) **Suspicious Transaction Report** means a report of the Company to the FIU of the activity or attempted activity that should be submitted by the Company no later than 5 working days if the Company knows or suspects that another person is engaged in money laundering or terrorism financing;

r) **FIU** means the Financial Intelligence Unit established by the Act.

s) **FSC or Commission** means the Financial Services Commission of Mauritius;

## 2. INTRODUCTION

GMBB Investment Ltd (the "Company"), a private company with limited liability and licensed as a Global Business Company is the holder of Investment Dealer Licence with License no GB22201139 pursuant to section 29 of the Securities Act 2005, Rule 4 of the Securities (Licensing) Rules 2007 and Financial Services (Consolidated Licensing and Fees) Rules 2008.

The Company encourages at all times high standards of business and personal conduct. The Manual sets the appropriate framework to detect any risk of failure by the Company to comply with its obligations under the Act and Regulations, as well as the associated risks, and put in place adequate measures and procedures designed to minimise such risks. In addition, the Manual is designed to provide the necessary guidelines for the application of 'Know Your Customer' ("KYC") principles and the conduct of due diligence checks on prospective customers and transactions, fixes responsibility for the reporting of suspicious transactions and brings together the relevant compliance policies, rules, regulations that affect the Company's business activities.

It is the responsibility of Company's personnel to familiarise itself with the Manual and with any amendments which may be circulated from time to time. The Company places extreme importance on compliance with the laws and regulations and corporate policies which affect the business with which it is involved. When the personnel within the Company becomes aware of breaches of law, internal and or external regulations including the Manual, they should immediately bring this to the attention of the Compliance Officer..

This Manual has been prepared in accordance with the provisions of the Financial Intelligence and Anti-Money Laundering Act 2002 (the "FIAMLA"), the Financial Intelligence and Anti-Money Laundering Regulations 2018 (the "FIAMLR"), the Prevention of Terrorism Act 2002, the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019, the Anti-Money Laundering and Countering the Financing of Terrorism Handbook 2020 (the "FSC Handbook"), internationally recognized principles, any code, direction or guideline issued by the FSC or other competent authority as well as the Securities (Licensing) Rules 2007 as amended from time to time and the Financial Services Act 2007 ("FSA") and the United Nations (Financial Prohinitions, Arms Embargo and Travel Ban) Sanctions Act 2019("UNSA")

The Company reserves the right to make changes to the Manual from time to time and notification will be given to the relevant personnel of any changes.

## 3. BOARD OF DIRECTORS RESPONSIBILITY FOR COMPLIANCE

The Board of the Company ("Board") is responsible for managing the Company effectively and is in the best position to understand and evaluate all potential risks, including those of ML and TF. The Board must therefore take ownership of, and responsibility for, the business risk assessments and ensure that they remain up to date and relevant. On the basis of its business risk assessment, the Board must establish a formal strategy to counter money laundering and financing of terrorism and proliferation.

The Board shall have the ultimate responsibility for the effective management of the Company and compliance with applicable laws and regulations. More particularly, the Board shall:

a) have broad oversight on compliance with the provisions of this policy and providing guidelines regarding the management of AML/CFT compliance risks on a risk based approach;

b) ensure that systems and controls are appropriately designed, documented and implemented, and are effectively operated to reduce the risk of the business being used in connection with AML/CFT;

c) appoint all relevant officers required under the relevant AML/CFT regulations including a compliance officer (CO), a money laundering reporting officer (MLRO) and a deputy money laundering reporting officer (DMLRO);

d) be responsible for reviewing and making decisions, based on quarterly reports received on AML/CFT matters;

e) devise screening procedures to ensure high standards when hiring employees;

f) implement an ongoing training programme for its directors, officers and employees, as applicable, to maintain awareness of the Relevant Laws; and

g) appoint an independent audit function to test the policies, procedures and controls of the Company regarding AML/CFT.

The board and management have a responsibility to ensure that the Company's systems and controls are appropriately designed and implemented, and are effectively operated to reduce the risk of the business being used in connection with ML/TF.

The board or management of the Company must establish documented systems and controls which:

(a) undertake risk assessments of its business and its customers;

(b) determine the true identity of customers and any beneficial owners and controllers;

(c) determine the nature of the business that the customer expects to conduct and the commercial rationale for the business relationship;

(d) require identification information to be accurate and relevant;

(e) require business relationships and transactions to be effectively monitored on an ongoing basis with particular attention to transactions which are complex, both large and unusual, or an unusual pattern of transactions which have no apparent economic or lawful purpose;

(f) compare expected activity of a customer against actual activity;

(g) apply increased vigilance to transactions and relationships posing higher risks of ML/TF;

(h) ensure adequate resources are given to the CO to enable the standards to be adequately implemented and periodically monitored and tested;

(i) ensure procedures are established and maintained which allow the Money Laundering Reporting Officer ('MLRO') and the Deputy MLRO to have access to all relevant information, which may be of assistance to them in considering suspicious transaction reports ("STRs");

(j) require a disclosure to the Financial Intelligence Unit ("FIU") when there is knowledge or suspicion or reasonable grounds for knowing or suspecting ML and/or TF, including attempted ML and/or TF; and

(k) maintain records for the prescribed periods of time.

# 4. COMPLIANCE FUNCTION

## 4.1 Compliance Officer

In accordance with Article 22 (1) (a) of Regulations the Company shall designate a CO at senior management level and approved as officer under Section 24 of the FSA.

The CO is responsible for the implementation and ongoing compliance of the financial institution with internal programmes, controls and procedures with the requirements of the applicable regulations.

The CO appointed by the financial institution must:

(a) be a natural person;

(b) be of at least senior management level as defined under Regulations;

(c) be an approved officer under Section 24 of the FSA; and

(d) have the appropriate qualification knowledge, skill and experience to fulfil a compliance role within the Company.

The Company must ensure that the CO:

(a) has timely and unrestricted access to the records of the Company;

(b) has sufficient resources to perform his or her duties;

(c) has the full co-operation of the Company;

(d) is fully aware of his or her obligations and those of the financial institution; and

(e) reports directly to, and has regular contact with, the Board so as to enable the Board to satisfy itself that all statutory obligations and provisions in applicable legislative framework are being met and that the Company is taking sufficiently robust measures to protect itself against the potential risk of being used for ML and TF.

The functions of the CO include:

(a) ensuring continued compliance with the requirements of the applicable legislative framework subject to the ongoing oversight of the Board of the Company and management;

(b) undertaking day-to-day oversight of the program for combatting money laundering and terrorism financing;

(c) regular reporting, including reporting of non-compliance, to the Board and management; and

(d) contributing to designing, implementing and maintaining internal compliance manuals, policies, procedures and systems for combatting money laundering and terrorism and proliferation financing.

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

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

### 4.2 Money Laundering Reporting Officer ("MLRO")

In accordance with Article 26(1) of Regulations as well as the Handbook, the Company shall appoint a MLRO to whom an internal report shall be made of any information or other matter which comes to the attention of any person handling a transaction and which, in the opinion of the person gives rise to knowledge or reasonable suspicion that another person is engaged in money laundering or the financing of terrorism or proliferation.

The MLRO shall:

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

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

The Company should take appropriate measures to ensure that internal suspicious transaction reporting systems continue to function properly.

In the absence of the MLRO, the FSC requires the appointment of a Deputy MLRO who should be of similar status, qualification and experience to the MLRO.

Where a person is appointed as MLRO or a Deputy MLRO in various entities, the Company must ensure that there are adequate measures in place to ensure that:

- they have adequate autonomy and independence;
- they have access to all relevant material in order to make an assessment as to whether the transaction/activity is suspicious or not; and

- there is adequate reporting to the board of the entities.

The MLRO appointed by the Company must:

- be a natural person;
- be an approved officer under Section 24 of the FSA; and
- have the appropriate knowledge, skill and experience.

The Company must ensure that the MLRO:

- is the main point of contact with the FIU in the handling of disclosures;
- has unrestricted access to the CDD information of the financial institution's customers, including the beneficial owners thereof;
- has sufficient resources to perform his or her duties;
- is available on a day-to-day basis;
- reports directly to, and has regular contact with, the Board or equivalent of the Company; and
- is fully aware of both his or her personal obligations and those of the applicable legislative framework.

Approval of the appointment of the MLRO and the DMLRO

The Company shall seek prior approval of the Commission for the appointment of a MLRO and DMLRO. The appointment of an officer without approval is deemded to be of no effect as per Section 24 of the Financial Services Act 2007 ("FSA 2007"). The approval of the MLRO or the DMLRO shall be deemed to be approved where the Financial Services Commission has not objected to the proposal within 15 days of having received the application, or any information required under the FSA 2007, whichever is later.

**Role and duties of the Money Laundering Reporting Officer**

The duties of the MLRO should at a minimum consist of the following:

(a) Receiving internal suspicious transactions reports ("STRs"), reviewing, assessing and investigating the internal STRs in view of determining whether an external STR should be disclosed to the FIU;

(b) maintaining all related records;

(c) giving guidance on how to avoid tipping off the customer if any disclosure is made;

(d) acting as a main point of conytact between the FIU and the National Sanctions Secretariat and if required the FSC;

(e) keeping abreast of developments in relation to AML/CFT requitements (both locally and internationally); and

(f) providing reports and other information to senior management.

The MLRO shall be preparing reports annually or such other periodic reports as he/she deems necessary to the Board to report the number of internal reports made by staff, or the number of reports made to the FIU.

The MLRO should be the main point of contact with the FIU in the handling of disclosures. The Board of the Directors should have regular contact with the MLRO so as to ensure that the Company is:

- complying with all the statutory obligations and provisions regarding AML/CFT; and
- taking sufficiently robust measures to protect itself against the potential risk of being used for money laundering and terrorist financing.

In the absence of the MLRO, the Deputy MLRO is expected to fulfil similar duties, as provided and explained above.

### 4.3 Handling Customers' Complaints or Grievances/Internal Dispute Resolution policy

The CO is responsible for handling customers complaints or grievances. The duties of the CO includ e the effective and efficient handling of customers complaints or grievances so as to enable the Company to adopt and apply the required actions to prevent the repetition of the same complaints or grievances.

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

***Complaints Management procedure:***

The Company has to have in place the below described Complaints Management Procedure and to maintain a complaints folder, so as to ensure the timely recording of complaints and their on-going analysis for the tracing and managing of possible repeated systemic problems and if possible legal and operational risks:

- As a first step the CO should review the submitted complaint in order to prevent the repetition of the same complains or grievances.
- Upon review, the CO will record the complaints and inform the Customer accordingly.
- The CO shall investigate the information submitted by the Customer as the processing of the Complaint is subjected to the provision of the correct information by the Customer-Complainant.
- The CO will communicate in plain language and inform the Customer that the Company will take all the required actions to resolve the problem, and the approximate time required to do so.
- The required action, that lead to the solution of the complain/grievance, is taken by the Compliance function.
- The CO informs the Customer about the given solution to his/her complain/grievance.
- When providing a final decision that does not fully satisfy the complainant's demands, to notify in writing the complainant using a thorough explanation of its position on the complaint and set out the complainant's option to maintain the complaint.

The policy of the Company is to resolve the complaint/grievance within a reasonable time from the date of receipt of the complaint. In case, due to the nature of the complaint/grievance, more time is required then the CO should inform the Customer as to the reason why the Company has not been able to resolve the complaint and an estimated time to resolve the issue will be provided.

In general, the procedure followed by the Company in terms of Complaints handling should be in line with the below principles:

- Establishment of a simple and straightforward procedure easily understandable by customers.
- Customers to be treated in accordance with "Treating Customer Fairly" principle.
- The resolution of a complaint to be done within a reasonable time ensuring a fair and effective outcome.

If after 60 working days the Company has not satisfactorily addressed the issue of the complaint, then the complainant can bring the complaint to the FSC.

## 5. GENERAL PRINCIPLES FOR MARKET PRACTISE AND CODE OF CONDUCT

The Company has set forth the following principles that must be followed by all employees.

**Compliance with laws and regulations** - Conduct business in accordance with applicable laws and regulations.

**Integrity** - Conduct business high standards of integrity and fair dealing in the conduct of its business.

**Good faith, fair business conduct and equitable business practice** - Adopt measures for the safeguarding of the regular operation of the capital market and protection of customers' interests.

**Skill, Care and Diligence** - Conduct business with all due skill, professional care and diligence and effectively apply internal procedures towards its customers and other parties.

**Management and Control** - Take reasonable care to organise and control all affairs responsibly and effectively, by means of adequate management systems.

**Market Conduct** - Observe proper standards of market conduct in the market within which the Company operates.

**Obtain information about Customers** - Obtain adequate information in respect of the Company's customers prior to engaging into any contracts with them such as any information about their circumstances and financial objectives, which may be relevant to enable the Company to be in compliance with the Act and Regulations.

**Customers' Interests –** Pay due care to the interests of the Company's customers and treat them fairly.

**Communications with Customers** - Pay due care to the needs of the Company's customers, and communicate information to them in a way which is clear, fair and not misleading.

**Disclosure to Customers -** Take all steps necessary to give a customer information, in an understandable and timely way, all information to enable him to make a balanced and informed decision

**Duty not to mislead the Customers** - Avoid engaging into a conduct or course of action that may create a misleading impression to its customers.

**Confidentiality -** Confidentiality and customer anonymity are essential for preserving a reputable and efficient market place

**Conflicts of Interest** - Manage conflicts of interest fairly, both between the Company and its customers and between customers themselves end ensure fair treatment to all its customers by disclosure, internal rules of confidentiality, declining to act or otherwise.

**Prohibited Market Conduct** – Refrain from engaging in prohibited conducts such as market manipulation, misinformation and rumour; and insider dealing.

**Customers' Assets** – Ensure adequate protection for customers' assets held by the Company.

**Financial Resources** - Ensure that they maintain, at all times, adequate financial resources to meet their financial obligations and that they implement appropriate risk management policies in their business.

**Relationship with the FSC -** Deal with the Commission in a co-operative manner and must comply with their disclosure obligations in a prompt manner

## 6. DESCRIPTION OF MONEY LAUNDERING,TERRORIST AND PROLIFERATION FINANCING

Money laundering is a process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities. Money laundering enables criminals to maintain control over their illicit proceeds and ultimately to provide legitimate cover for the illegal source of the illicit proceeds. This means that proceeds from criminal activities is converted into assets that gives it an appearance of legitimate money. Money laundering is an international scourge and the failure by the authorities to prevent the laundering of the proceeds of crime will enable criminals to benefit from their illegal activities, thereby making crime a viable proposition.

The Financing of Terrorism is defined as an offence established when a person "by means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge

that they will be used in full or in part, in order to carry out a terrorist act or activity". Terrorist financing is a unique form of financial crime. Unlike money laundering, which is finding dirty money that is trying to be hidden; terrorist financing is often clean money being used for lethal purposes.

Proliferation of weapons of mass destruction ("WMDs") can be in many forms, but ultimately involves the transfer or export of technology, goods, software, services or expertise that can be used in programmes involving nuclear, biological or chemical weapons, and their delivery systems (such as long range missiles). Proliferation of WMD financing is an important element and, as with international criminal networks, proliferation support networks may use the international financial system to carry out transactions and business deals. Unscrupulous persons may also take advantage of the potential profits to be made by facilitating the movements of sensitive materials, goods, technology and expertise, providing seemingly legitimate front organisations or acting as representatives or middlemen.

The Company should follow and apply the provisions of the law which reflect the Financial Action Task Force's (FATF) international standards to prevent, detect and combat money laundering and terrorist financing. It is, therefore, imperative that all relevant personnel understand the nature of money laundering, terrorism and proliferation financing and take the necessary measures to protect themselves.

There is no specific method of laundering money. Despite the variety of methods employed, the laundering process is accomplished in three basic stages which may comprise transactions by the launderers that could alert a financial institution to criminal activity:

- **Placement:** is the physical deposit of criminal proceeds derived from illegal activity i.e. entering the collected cash into the financial circuits (payment in cash, exchange of bills, manual exchange, travelers' checks, casino checks, etc.).

- **Layering:** is the separation of criminal proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity i.e. transfer between accounts, drawing of checks, foreign transactions etc.

- **Integration:** is the provision of apparent legitimacy to the proceeds of crime. If the layering process has succeeded, integration places the laundered proceeds back into the economy in such a way that they appear as normal (business) funds or other assets i.e. investing funds in lawful investments (stores, leisure activities, real estate, but also companies of all types, etc.

**Offence of Money Laundering as per the Financial Intelligence and Anti-Money Laundering Act**

A person is guilty of money laundering if the person:

a) engages in a transaction that involves property which is, or in whole or in part directly or indirectly represents, the proceeds of any crime; or
b) receives, is in possession of, conceals, disguises, transfers, converts, disposes of, removes from or brings into Mauritius any property which is, or in whole or in part directly or indirectly represents, the proceeds of any crime,

where he suspects or has reasonable grounds for suspecting that the property is derived or realized, in whole or in part, directly or indirectly from any crime, shall commit an offence.

Any person engaged in money-laundering is guilty of an offence punishable on conviction by:

a) a fine not exceeding 10 million rupees and;
b) to penal servitude for a term not exceeding 20 years.

## 7. AML/CFT INTERNAL CONTROLS, POLICIES AND PROCEDURES

The Company has established internal controls, policies and procedures for the assessment of risks and the prevention of AML/CFT which are documented in this Manual in the following sections.

The AML and CFT Procedure Manual must contain internal policies, controls and procedures:

a) to mitigate and manage effectively the risks of money laundering and terrorism financing identified in any risk assessment undertaken;
b) to regularly review and update the established policies, controls and procedures;
c) maintain a record in writing of
    i. the established policies, controls and procedures;
    ii. any changes to those policies, controls and procedures made as a result of the review and update required; and
    iii. the steps taken to communicate those policies, controls and procedures, or any changes to them, internally.

**Note:**

The policies, controls and procedures adopted under paragraphs (a), (b) and (c) shall be proportionate to the size and nature of the business of a reporting person, as the case may be, and approved by its management.

In addition to that, the Company shall implement internal controls and other procedures to combat money laundering and financing of terrorism, which shall include:

a) programmes for assessing risk relating to money laundering and financing of terrorism;
b) the formulation of a control policy that will cover issues of timing, degree of control, areas to be controlled, responsibilities and follow up;
c) monitoring programmes in relation to complex, unusual or large transactions;
d) enhanced due diligence procedures with respect to persons and business relations and transactions carrying high risk and with persons established in jurisdictions that do not have adequate systems in place against money laundering and financing of terrorism and proliferation;

e) carry out screenings with respect to sanctions;

f) providing employees, including the Money Laundering Reporting Officer, from time to time with training in the recognition and handling of suspicious transactions;

g) making employees aware of the procedures under these regulations, the Act, Handbook and Guidelines and any other relevant policies that are adopted by the relevant person; and

h) establishing and maintaining a manual of compliance procedures in relation to AML/CFT.

## 7.1 Application of Appropriate Measures and Procedures on a Risk Based Approach

The Company applies appropriate measures and procedures, on a risk based approach, so as to focus its effort in those areas where the risk of money laundering and terrorist financing appears to be higher.

### 7.1.1 Risk Based Approach ("RBA")

In implementing a RBA, the Company implements processes to identify, assess, monitor, manage and mitigate money laundering and terrorist financing risks. The general principle of a RBA is that, where there are higher risks, the Company should take enhanced measures to manage and mitigate those risks; and that, correspondingly, where the risks are lower, simplified measures may be permitted. Simplified measures should not be permitted whenever there is a suspicion of money laundering or terrorist financing). More specifically, a RBA:

(a) identifies the specific threats posed to the Company by ML and TF and those areas of the Company's business with the greatest vulnerability;

(b) assesses the likelihood of those threats occurring and the potential impact of them on the Company;

(c) mitigates the likelihood of occurrence of identified threats and the potential for damage to be caused, primarily through the application of appropriate and effective policies, procedures and controls;

(d) manages the residual risks arising from the threats and vulnerabilities that the Company has been unable to mitigate; and

(e) allows the review and monitoring those risks to identify whether there have been any changes in the threats posed to the Company which necessitate changes to its policies, procedures and controls.

Moreover, when determining and putting in place appropriate risk-based systems and controls, the Company shall have regard to the nature, size and complexity of its business and the type of ML and TF risk that it might reasonably face in identifying its ML and TF risk, the Company must consider the risk posed by the following factors:

a. Its customer type, including any politically exposed persons;
b. The types of designated services it provides;
c. The methods by which it delivers designated services; and
d. The foreign jurisdictions with which it deals.

In addition to that the Company has put in place risk based systems and controls to deal with political exposed persons ("PEPs") who are customer and must include the enhanced customer identification process, enhanced customer verification and enhanced on-going due diligence processes.

In cases where a customer is regarded as higher risk, the company shall take reasonable steps to:

- Collect and verify additional information on the intended nature of the business relationship;
- Collect and verify information on the source of funds or source of wealth of the customer;
- Collect and verify information on the ultimate beneficial owner of the customer;
- Collect and verify information on the reason for intended or performed transactions;
- Obtaining the management's approval of the Company to commence or continue the business relationship; and
- Conduct regular and ongoing monitoring of the customer's transactions.

Also, the Company has in place appropriate risk-based systems and controls to identify, verify and understand whether the customer or the beneficial owner of the customer is a political exposed person or an immediate family member of a political exposed person or a close associate of a political exposed person.

### 7.1.2 Risk Assessment

The Company must complete a risk assessment to identify and measure the inherent risk of ML, TF and sanctions and evaluate the design and effectiveness of controls to determine the Company's residual risk.

The risk assessment must adequately account for the potential ML, TF and sanctions risk arising from all relevant factors, including the Company's customers, products, services, delivery channels, supply chain, intermediaries, counterparties, transactions and geographic locations. The risk assessment must also be proportionate to the size and complexity of the Company and its operations.

The risk assessment results inform the design, development, maintenance and implementation of its AML/CTF and sanctions policies and procedures and other mitigation activities in accordance with the National Money Laundering and Terrorist Financing Risk Assessment of Mauritius ("NRA Report").

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

(a) the nature, scale and complexity of the Company's activities;
(b) the products and services provided by the Company;
(c) the persons to whom and the manner in which the products and services are provided;
(d) the nature, scale, complexity and location of the customer's activities;
(e) reliance on third parties for elements of the customer due diligence process; and
(f) technological developments.

The Company must record and document its business risk assessment in order to demonstrate its basis. It should be reviewed at least once a year or shorter interval as may be required and updated as appropriate. The review needs to be documented to evidence that an appropriate review has taken place.

The business risk assessment and any review thereof shall take into account the findings of the National Risk Assessment and any guidance issued thereon.

While carrying out its Business Risk Assessment, all relevant departments should work together such that the exercise is comprehensive and addresses risks. Primarily, responsibility for risk analysis rests with the operations and business departments. The compliance department is responsible for the process monitoring, facilitating and testing. Ultimate responsibility for the Business Risk Assessment rests with the Board of Directors.

### 7.1.3 Identification and Evaluation of Risks

The identification and assessment of risk can be addressed through the following questions:

a. What risk is posed by the Company's customers?
b. What risk is posed by a Customer's behaviour?
c. How did the Customer communicate with the Company?
d. What risk is posed by the services and financial instruments provided to the Customer?

- <u>What risk is posed by the Company's customers?</u>

The following should be taken into consideration (List not exhaustive):

a. Non-face-to-face customers;
b. Complexity of ownership structure of legal persons;
c. Companies with bearer shares;
d. Politically Exposed Persons; and
e. Customers from high risk countries or from countries known for high level of corruption or organized crime or drug trafficking.

- <u>What risk is posed by a Customer's behaviour?</u>

The following should be taken into consideration (List not exhaustive):

a. Customer transactions where there is no apparent legal financial/commercial rationale;
b. Situations where the origin of wealth and/or source of funds cannot be easily verified; and

c. Unwillingness of customers to provide information on the Beneficial Owners of a legal person.

- How did the Customer communicate with the Company?

The following should be taken into consideration (List not exhaustive):

a. Non-face to face customer; and
b. Customer introduced by a third person.

- What risk is posed by the services and financial instruments provided to the Customer?

The following should be taken into consideration (List not exhaustive):

a. Services that allow payments to third persons; and
b. Large cash deposits or withdrawals.

- Does the Company apply appropriate measures and what parameters shall the Company consider?

Indicative parameters are the following:

a. The scale and complexity of the services;
b. Geographical spread of the services and Customers;
c. The nature (e.g. non-face to face Customer) and economic profile of customers as well as of financial instruments and services offered;
d. The distribution channels and practices of providing services;
e. The volume and size of transactions;
f. The degree of risk associated with each area of services;
g. The country of origin and destination of customers' funds;
h. Deviations from the anticipated level of transactions; and
i. The nature of business transactions.

After collection of all CDD documentation, the Company shall undertake an initial assessment of the risk to which the business relationship will expose the Company and evaluate the customer accordingly. The risk profiling tool helps the Company evaluate potential AML/CFT risks in relation to a potential client, with specific weightage allocated to each factor done on an automated basis. Clients are then classified as a High Risk, Medium Risk or Low Risk.

In this exercise, the Company shall take into consideration a number of factors, including but not limited to the following:

- The nature and type of customer, his present occupation and career history
- The commercial rationale for the relationship
- The geographical location of the customer's residence
- The geographical location of the customer's business interests and/or assets
- The nature and value of the assets concerned in the relationship
- The customer's source of funds and where necessary the source of wealth
- any adverse information or hit

The risk profiling sheet shall be completed each time there is new client relationship or there is a change in any of the risk variables. Once the business is up and running, the Company shall monitor, on an on-going basis, that 'risk profile' by scrutinising the various transactions entered into by the client, for instance, by reviewing all bank statements and by keeping an eye on the relationship as a whole so as to ensure that it is consistent with the Company's knowledge of the customer, of the latter's 'risk profile' and source of funds. The Company shall set the frequency of the review of a specific relationship based on the risk profile of the customer relationship.

### 7.1.4 Weightage of Risk Factors

When weighting risk factors, the Company should ensure that:

(a) weighting is not unduly influenced by just one factor;

(b) economic or profit considerations do not influence the risk rating;

(c) weighting does not lead to a situation where it is impossible for any business relationship or occasional transaction to be classified as a high risk relationship;

(d) the provisions of Article 12(1) of Regulations setting out the situations which will present a high risk (for example, the involvement of PEPs or in event of suspicious activity) cannot be over-ruled by the Company's weighting; and

(e) it is able to override any automatically generated risk scores where necessary. The rationale for the decision to override such scores should be documented appropriately.

### 7.1.5 Business Risk Assessment

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

(g) the nature, scale and complexity of the Company's activities;

(h) the products and services provided by the Company;

(i) the persons to whom and the manner in which the products and services are provided;

(j) the nature, scale, complexity and location of the customer's activities;

(k) reliance on third parties for elements of the customer due diligence process; and

(l) technological developments.

**The nature, scale and complexity of its activities**

- Consider the services provided by the business and how those services might be abused for ML/TF.
- Actively involve all members of management in determining the risks (threats and vulnerabilities) posed by ML/TF within those areas for which they have responsibility.
- Consider any organisational factors that may increase exposure to the risk of ML/TF e.g. business volumes and outsourcing aspects of regulated activities or compliance functions.
- Consider the nature, scale and complexity of its business including the diversity of its operations, the volume and size of its transactions, and the degree of risk associated with each area of its operation. Large

volume and more complex transactions may pose higher risk of money laundering than less complex and voluminous transactions.

- Consider the jurisdictions in which the business operates, any particular threats from those jurisdictions, any particular vulnerabilities within the organisation in those jurisdictions. Article 24(1) of the Regulations states how high risk countries should be identified.

**The products and services provided by the Company**

- Consider the vulnerabilities of the services or products offered and how they could be abused for ML/TF.
- Certain characteristics of the products and whether there are any increased vulnerabilities such as high volumes of cash, virtual currencies or untraceable/anonymous medium.
- Whether payments to any unknown or un-associated third parties are allowed. Such payments would entail higher risks.
- Whether the products/services/structure are of particular, or unusual complexity.

**The persons to whom and the manner in which the products and services are provided**

- Consider the threats posed by the types of customers. Some examples include, politically exposed persons ("PEPs"); high net worth individuals, those from or operating in a higher risk jurisdiction; and non-face- to-face business.
- The type of product should be considered, the higher risk products or services are more likely to be those with high values and volumes; where unlimited third party funds can be freely received and those where funds can regularly be paid to third parties without CDD on the third parties being obtained.
- The speed with which products and services can be delivered or transactions undertaken.

**The nature, scale, complexity and location of the customer's activities**

- Whether the customer base has any involvement in those businesses which are likely to be most vulnerable to corruption, such as oil, construction or arms sales.

- Consider jurisdictional factors such as high levels of organised crime, increased vulnerabilities to corruption and inadequate frameworks to prevent and detect ML/TF in countries where it may have customers.
- The countries, territories and geographic areas with which customers (and the beneficial owners of customers) have a relevant connection.

**Reliance on third parties for elements of the customer due diligence process**

The Company may rely on a third party to introduce business or to perform the CDD measures. When reliance is placed on third parties, the following may be considered:

- Consider how reliance on third parties is prompted and agreed on.
- Consider who these third parties are, including any reputational issues, the quality of relationships with such third parties and previous experiences.
- Consider the extent and type of any reliance placed or to be placed on third parties.
- Consider the extent of the information being provided by the third party and who has actually met the customer face-to-face (chains of information).
- Consider any jurisdictional issues in connection with reliance placed on third parties.
- Consider the results of any testing undertaken on the third party's procedures and the responses to any previous requests for documentation.
- Consider the extent of any outsourcing undertaken.
- Consider the quality of the provider for any outsourced functions including any reputational issues, previous experiences with the provider, results of any audits, assessments or inspections where the material generated as a result of outsourcing has been reviewed.

The Company should also establish procedures to be satisfied that:

- the third party applies CDD measures and keeps records to a standard equivalent to the FATF Recommendations;
- the third party will provide, immediately upon request, relevant copies of identification data in accordance with applicable legislative framework; and
- the quality of the third party's CDD measures is such that it can be relied upon.

**Technological developments**

The Company should assess the use of developing technologies for both new and pre-existing products such as:

- digital information storage including cloud computing;
- digital or electronic documentation storage;
- electronic verification of documentation;
- data and transaction screening systems; or
- the use of virtual or digital currencies, if applicable.

For completeness, the assessment should consider the operational risks, reputational risks and legal risks posed by the use of new technologies in the context of ML/TF. Appropriate action should be taken to mitigate the risks that have been identified.

### 7.1.6 List of Risk Rating for Countries and Jurisdictions

This particular list is a complex and comprehensive list which has as source lists the following:

- The FATF Listing
- The FSC List of Equivalent Jurisdictions
- The Corruption Perception Index
- The Basel AML Index
- Sanction Lists (EU, UN and US)
- The International Narcotics Control Strategy Report on Countries

The Company applies the highest rating of all the above lists to its Country List. This list is consulted in various situations such as:

- When establishing a client's country of origin, of operations and source of funds & wealth
- When establishing the countries of operations
- During the course of a client relationship, whenever a cross border transaction has to be executed.

This list identify risk elements, evaluate the feasibility of certain transactions and to apply such measures as

necessary to mitigate the risks, if applicable. The List of Risk Rating for Countries and Jurisdictions is reviewed on a monthly basis and if updates are available for the source lists, then same is reflected in the internal list.

### 7.1.7 Risk Categorisation

**The risk categorisation is as follows:**

| Low Risk | Medium Risk | High Risk |
|---|---|---|
| ✓ Clean independent verification<br>✓ No matters of concern identified<br>✓ All KYC on record<br>✓ The evaluation shows that there is minimum to no risk in terms of managing the client relationship and the operations of the structure | ✓ Moderate information in terms of independent verification<br>✓ Some element of risks identified but which are deemed under control and well mitigated | ✓ High elements of risks identified in terms of checks and verification<br>✓ Nature of the business activity may be deemed as potentially high risk<br>✓ Client may be a High Profile Individual ("HPI") or PEP but with no adverse report<br>✓ Strict parameters are set for the duration of the client relationship and monitored at all times. |

**A Customer Risk Assessment shall be conducted each time there is new client relationship or there is a change in any of the risk variables.**

**There shall be monitoring, on an ongoing basis of that 'risk profile' by scrutinising the various transactions entered into by the client, for instance, by reviewing all bank statements and by keeping an eye on the relationship as a whole so as to ensure that it is consistent with the Company's knowledge of the customer, of the latter's risk profile and source of funds.**

**Note: The Company shall set the frequency of the review of a specific relationship based on the risk profile of the customer relationship. High Risk on an annual basis(earlier in case of trigger events), Medium every 2 years (earlier in case of trigger events) and Low every 4 years (earlier in case of trigger events).**

### 7.1.8 Risk Factors

The following risk factors are examples of factors that the financial institution shall consider when undertaking a risk assessment of the relationship they have with their customers. These factors aim the Company to assess and decide what is appropriate in the circumstances of the business relationship and it is not expected that all factors will be considered in all cases. The risk factors are defined as follows:

a) Customer Risk Factors;
b) Countries and Territories Risk Factors;
c) Products, Services and Transactions Risk Factors

Examples of the above risk factors can be found in **Annex I**.

### 7.1.9 A Risk Weightage Analysis and Methodology

The Company uses the risk scoring tables below to weigh the risk assessment of the AML/CFT BRA.

| SCORE | RISK WEIGTAGE |
|---|---|
| 1 | Low |
| 2 | Medium |
| 3 | Medium-High |
| 4 | High |

**Business Risk Assessment Methodology**

Below is a description on how different variables are defined and the sources of data to be used for rating purposes.

| Variable | Factors | Data source |
|---|---|---|
| The nature, scale, and complexity of the reporting person's activities. | • Diversity of operations.<br>• Outsourcing of functions.<br>• Volume and size of transactions. | • Business plan/PPM<br>• Management agreement/services agreements.<br>• Bank statements. |
| The products and services provided by the reporting person. | • The product or service provided.<br>• Complexity of product.<br>• Payment to unknown or un-associated third parties.<br>• The delivery channel – to consider the use of introducers.<br>• Target markets. | • Business plan/PPM.<br>• Bank statements. |
| The persons to whom and the manner in which the products and services are provided. | • PEPs.<br>• Adverse reports.<br>• Identification of beneficial owners of customers.<br>• Jurisdictions under increased monitoring<br>• Third party transactions (funding).<br>• Customer Due Diligence Documents. | • PEP Register.<br>• Bank statements.<br>• Agreements.<br>• Customer Due Diligence Documents |
| The nature, scale, complexity, and location of the customer's activities. | • Customers' relationship with high business activities such as oil or arms sales.<br>• Customers' connection with high jurisdictions | • Profile of customers. |

| | | |
|---|---|---|
| Reliance on third parties for elements of the customer due diligence process | • Third party's jurisdiction.<br>• Testing of third-party relationship. | • Profile of third party.<br>• Testing |
| Technological Developments | • Electronic verification of documents.<br>• Use of virtual currencies.<br>• Digital information storage .<br>• Data and transaction screening systems. | • Procedures manual. |

### 7.1.10 International AML/CFT Initiatives

For the implementation of appropriate measures and procedures on a risk-based approach, the Compliance Function ensures that they consult, among others, the recommendations and consultations of the following relevant international organisations:

- Financial Action Task Force (FATF), www.fatf-gafi.org
- Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), http://www.fatf-gafi.org/countries/#ESAAMLG
- Basel Committee on Banking Supervision - https://www.bis.org/
- International Organisation of Securities Commissions (IOSCO) – www.iosco.org
- The Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) - www.coe.int/moneyval
- The UN Security Council Sanctions Committees - www.un.org/sc/committees/
- The International Monetary Fund (IMF) – www.imf.org
- National Money Laundering and Terrorist Financing Risk Assessment of Mauritius (NRA Report)- https://www.fscmauritius.org/en/being-supervised/amlcft/national-money-laundering-and-terrorist-financing-risk-assessment-of-mauritius-nra-report

### 7.2 Customer Identification and Due diligences procedures ("CDD")

The CDD procedure has the following meaning:

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

The Company must ensure that all documents, data or information collected under the CDD process are kept relevant and up-to-date by undertaking reviews of existing records, using a risk based approach particularly for higher risk categories of customer or business relationships.

In the case where the Company form a suspicion that transactions related to money laundering or terrorist financing, they should take into consideration the risk of tipping off when performing the customer due diligence process. If the Company reasonably believes that performing the CDD process will tip-off the customer or potential customer, it may choose not to pursue that process, and should file Suspicious Transactions Report (STR) to the FIU as described in section 6.5 of the Code.

Finally, it's the Company's duty to ensure that their employees are aware of and sensitive to these issues when conducting CDD.

#### 7.2.1 Obligations for customer identification and due diligence procedures

The Company must carry out a CDD identification process in the following circumstances:

- When opening an account for, or otherwise establishing a business relationship with, a customer;
- Where a customer who is neither an account holder nor in an established business relationship with the reporting person wishes to carry out –
    (i) a transaction in an amount equal to or above 500, 000 rupees or an equivalent amount in foreign currency or such amount as may be prescribed, whether conducted as a single transaction or several transactions that appear to be linked; or
    (ii) a domestic or cross-border wire transfer;
- Whenever doubts exist about the veracity or adequacy of previously obtained customer identification information; and
- Whenever there is a suspicion of money laundering or terrorism financing involving the customer or the customer's account.

In respect to every single customer and business relationship, the Company shall, when applying CDD measures, take into account the outcome of the risk assessment required to be carried out.

Also, in case where the risks are higher, a reporting person shall conduct enhanced due diligence measures consistent with the risks identified. In the other case where the risks are lower, a reporting person may conduct simplified due diligence measures. Unless there is a suspicion of money laundering or terrorism financing in which case enhanced CDD measures shall be undertaken.

In all cases, the Company shall apply such CDD measures as may be prescribed and/or specified by the competent authority.

### 7.2.2 Ongoing Monitoring

Once the identification procedures have been completed and the business relationship has been established, the Company must undertake on-going due diligence process to monitor its account, service or relationship with each of its customers to identify, mitigate and manage the risk it may reasonably face with its customers that might involve money laundering, financing of terrorism or other serious offences.

For effective ongoing monitoring, the Company considers:

a. 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 Company'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 Company 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.

The Company shall conduct ongoing monitoring of a business relationship by:

a. scrutinising transactions undertaken throughout the relationship to ensure that the transactions are consistent with the Company's knowledge of the customer, the business and risk profile and the source of funds of the customer; and
b. keeping the documents, data or information obtained for the purpose of applying customer due diligence measures up to date.

Moreover, by monitoring the customer's activities and transactions, the Company must execute periodic reviews using a risk-based approach of the existing records and ensuring that up-to date information is held in relation to the business relationship. In the same manner, the Company shall put in place appropriate risk-based systems and controls to determine whether any further customer information (including updating existing information) is required for its ongoing due diligence purposes:

a) **Transaction Monitoring process** – the Company has in place a transaction monitoring system to scrutinize transactions that are inconsistent with information held about the business relationship with the Company. The transaction monitoring system shall identify any transaction that appears to be suspicious, complex, unusual, and have no apparent visible economic or lawful purpose.

   The objective is to set out an effective transactions monitoring mechanism and ensuring that any Money laundering and Terrorist Financing risks are identified at the outset and are mitigated. In that respect, the following has been implemented:

i. All transactions will need to be entered into a Transactions Monitoring Checklist ("TMC") where extensive monitoring must be conducted by operations teams on all transactions (including but not limited to bank transactions) to verify source and destination of funds (special attention to PEP's) and ascertain whether such transactions are in line with the entities' business activities. The transactions should also be properly supported/evidenced;

ii. The TMC needs to be filled in by the relevant administrator, reviewed and approved by two senior officers (a Reviewer reviews and an Approver approves the TMC).

iii. A transaction monitoring register should be kept where all transactions must be properly monitored and the register completed and signed off by a senior officer on a monthly basis after having verified the relevant bank statements.

iv. A TMC should be escalated for approval to the Senior Management/CO in the followi ng situations:

- Transactions above the agreed monetary threshold;
- Transaction not in line with the business activities of the entity of the Company;
- Transactions involving PEPs; and
- Transactions involving sanctioned country(ies).

The above monitoring procedures caters for both real-time and post-event monitoring.

In case any matter of concern in relation to the payment is identified or the supporting documents or due diligence are unsatisfactory, the transaction will be placed on hold until the transaction and supporting documents are re-evaluated and are deemed to be in full compliance with all the regulatory requirements.

b) Customer Monitoring Process – the Company shall have a customer monitoring process where it can monitor its relationship with its customer to ensure that the customer's activities being conducted is consistent with its knowledge of the customer, the customer's business, source of funds and risk profile;

c) Enhanced Customer Due Diligence process –the Company shall apply the enhanced customer due diligence program when:

   i. it determines under its risk-based systems and controls that the ML and TF risk is high; or

   ii. a suspicious transaction or activity or a transaction conducted by money laundering entities or a transaction involving terrorist property or a transaction with no legitimate purpose has arisen; or

   iii. a party to the transaction, which the Company is entering into or proposing to enter into, is physically present in, or is a business incorporated in, a prescribed foreign country.

In addition, the Company must include one or more of the following when undertaking appropriate risk-based systems and controls:

a) regularly collect information from the customer or from third party sources in order to update its knowledge (derived from the enhanced identification process) of the customer;
b) undertake more detailed analysis of the customer information including examining as far as possible the background and purpose of the transaction and business relationship;
c) regularly verify or re-verify the customer information in accordance with the customer identification process; and
d) undertake more detailed analysis and monitoring of the customer's transactions - both past and future, including, but not limited to:

   i. the purpose or nature of specific transactions; or

   ii. the expected nature and level of transaction behaviour;

The aim of the ongoing monitoring rules is to have a full understanding of normal and reasonable account activity of the Company's customers as well as of their economic profile and have the means of identifying transactions which fall outside the regular pattern of an account's activity or to identify complex or unusual transactions or transactions without obvious economic purpose or visible legitimate reason. Without such knowledge, the Company will not be able to discharge its legal obligation to identify and report suspicious transactions to FIU.

Although, not all the unusual or unexpected activity is necessarily suspicious. For this reason, the employees are expected to be able to recognise unusual activity resulting from the effective CDD checks conducted on an on-going basis.

The monitoring of accounts and transactions are carried out in relation to specific types of transactions and economic profile, as well as by comparing periodically the actual movement of the account with the expected turnover as declared at the establishment of the Business Relationship.

The Company introduces and implements, where appropriate and proportionate, adequate automated electronic management information systems which will be capable of supplying the dedicated personnel, on a timely basis, all the valid and necessary information for the identification, analysis and effective monitoring of Customer accounts and transactions based on the assessed risk for money laundering or terrorist financing purposes. The automated electronic management information systems may also be used to extract data and information that is missing regarding the Customer identification and the construction of a Customer's economic profile.

For all accounts, automated electronic management information systems are able to add up the movement of all related accounts on a consolidated basis and detect unusual or suspicious activities and types of transactions. This can be done by setting limits for a particular type, or category of accounts (e.g. high risk accounts) or transactions (e.g. deposits and withdrawals in cash, transactions that do not seem reasonable based on usual business or commercial terms, significant movement of the account incompatible with the size of the account balance), taking into account the economic profile of the Customer, the country of his origin, the source of the funds, the type of transaction or other risk factors. The Company gives particular attention to transactions exceeding the abovementioned limits, which may indicate that a Customer might be involved in unusual or suspicious activities. Section 12(2)(f) of Regulations 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 Regulations requires a financial institution 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:

- undertaking more frequent reviews of high risk relationships and updating CDD information on a more regular basis;
- undertaking more regular reviews of transactions and activity against the profile and expected activity of the business relationship;
- applying lower monetary thresholds for the monitoring of transactions and activity;
- reviews being conducted by persons not directly involved in managing the relationship for example, the CO;
- ensuring that the financial institution 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;
- appropriate approval procedures for high value transactions in respect of high risk relationships; and/or
- a greater understanding of the personal circumstances of high risk relationships, including an awareness of sources of third party information.

**High Risk Transactions or Activity and Ongoing Monitoring**

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

a. an unusual transaction in the context of the financial institution'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);
b. funds originating from, or destined for, an unusual location, whether specific to an individual business relationship, or for a generic customer or product type;
c. transactions or activity unexpectedly occurring after a period of dormancy;
d. unusual patterns of transactions or activity which have no apparent economic or lawful purpose;

e. an instruction to effect payments for advisory or consulting activities with no apparent connection to the known activities of the customer or their business;
f. the involvement of charitable or political donations or sponsorship;
g. a relevant connection with a country or territory that has significant levels of corruption or provides funding or support for terrorist activities;
h. Identification of a PEP or a high profile individual; or
i. Connected persons that are PEPs.

**FATF Statements and non-cooperative jurisdictions**

For the design of internal procedures, the Company must have regard to the need of enhanced due diligence and additional monitoring procedures for transactions and business relationships involving countries which are non-cooperative jurisdictions, or which have been the subject of FATF Public Statements for deficiencies in their AML/CFT systems. (Please refer to **Annex II**)

**Timing of identification and verification process:**

The Company must take all reasonable measures to complete all CDD measures for all applicants for business prior to the establishment of a new customer relationship and prior to providing any financial service.

Where it is necessary to provide financial services to an applicant for business prior to completion of CDD measures, the decision to do so must be appropriately authorised by senior management and the reasons recorded in writing.

The CDD measures must in any event be satisfactorily completed, such that:

a. it occurs as soon as reasonably practicable;
b. it is essential not to interrupt the normal conduct of business; and
c. the money laundering risks are effectively managed.

Examples of situations where verification of identity may be delayed provided that, inter alia, this does not interrupt the normal course of business are:

- Non-face-to-face business
- Securities transactions

The Company must have appropriate and effective policies, procedures and controls in place, so as to manage the risk, which must include:

a. establishing that the transaction is not a high risk relationship;
b. monitoring by management of these business relationships to ensure that the verification of identity is completed as soon as reasonably practicable;
c. ensuring funds received are not passed on to third parties;
d. establishing procedures to limit the number, types and/ or amount of transactions that can be undertaken; and
e. monitoring large or complex transactions.

In the event that satisfactory CDD documentation has not been obtained, the Company must have procedures in place to disengage from or terminate such business relationships and consider making a suspicious transaction report.

Where the Company is unable to comply with the CDD requirements with respect to an applicant for business, it should consider making a suspicious transaction report to the FIU.

### 7.3 Construction of Economic profile

For the construction of a Customer's Economic profile the following rules shall be always adopted:

1. The Company must be satisfied that it's dealing with a real person and, for this reason, obtains sufficient evidence of identity to verify that the person is who he claims to be. Furthermore, the Company must

verify the identity of the beneficial owners of the Customers' accounts. In the cases of legal persons, the Company obtains adequate data and information so as to understand the ownership and control structure of the Customer. Irrespective of the Customer's type, the Company requests and obtains sufficient data and information regarding the Customer's business activities and the expected pattern and level of transactions.

2. The verification of the customers' identification is based on reliable data and information issued or obtained from independent and reliable sources, meaning data, and information that are the most difficult to be amended or obtained illicitly.

3. A person's residential and business address is an essential part of his identity.

4. It is not acceptable to use the same verification data or information for verifying the Customer's identity and verifying its home address.

5. The data and information that are collected before the establishment of the Business Relationship, with the aim of constructing the Customer's economic profile and, as a minimum, include the following:
   i. the purpose and the reason for requesting the establishment of a Business Relationship;
   ii. the anticipated account turnover, the nature of the transactions, the expected origin of incoming funds to be credited in the account and the expected destination of outgoing transfers/payments; and
   iii. the Customer's size of wealth and annual income, and the clear description of the main business/professional activities/operations.

6. The data and information that are used for the construction of the Customer's economic profile include, inter alia, the name of the company, the country of its incorporation, the head offices address, the names and the identification information of the Beneficial Owners, directors and authorised signatories, financial information (latest financial statements, and if not applicable, then management accounts) and ownership structure of the group that the company may be a part of (country of incorporation of the

parent company, subsidiary companies and associate companies, main activities and financial information).

7. The said data and information are recorded in a separate form designed for this purpose which is retained in the Customer's file along with all other documents as well as all internal records of meetings with the respective Customer.

8. The said form is updated regularly or whenever new information emerges that needs to be added to the economic profile of the Customer or alters existing information that makes up the economic profile of the Customer.

9. Identical data and information with the above mentioned are obtained in the case of a Customer-natural person, and in general, the same procedures with the above mentioned are followed.

10. Transactions executed for the Customer are compared and evaluated against the anticipated account's turnover, the usual turnover of the activities/operations of the Customer and the data and information kept for the Customer's economic profile. Significant deviations are investigated and the findings are recorded in the respective Customer's file.

11. Transactions that are not justified by the available information on the Customer, are thoroughly examined so as to determine whether suspicions over money laundering or terrorist financing arise for the purposes of submitting a Suspicious Transaction Report to FIU.

### 7.4 Third party reliance for verification process (Refer to Annex IX on Template Third Party Reliance Template)

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 financial institution must ensure that the identification information sought from the third party is adequate and accurate.

The CDD information has to be submitted immediately in line with section 17D of the Act upon on boarding 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 Company 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 Act and record keeping requirements pursuant to section 17F of the Act and Article 21 of the Regulations which provides for third party reliance.

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

The Company should also ensure that:

- there is a signed agreement 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 on boarding;
    - 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;
    - the signed agreement does not contain any conditional language, whether explicit or implied, which may result in the inability of the third party to provide the CDD documents; 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.

## 7.5 Identification and Verification procedures

### 7.5.1 Customers' Due Diligence measures

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

- Identification data for natural persons:

- Name (including any former names, any other names used and other aliases)
- Sex
- Current residential address
- Permanent residential address (if different to current residential address)
- Date and place of birth
- Nationality
- Any occupation, public position held and where appropriate the name of the employer
- Government issued personal identification number or other government issued unique identifier

- Verification methods of the Identity of the natural person:

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

All identification data collected by the Company must be verified.

In addition to that, the identity documentation must be obtained and retained by the Company to verify the information provided by principals about their identity. The documentation must be pre-signed and must be either in an original form or must be certified appropriately – and should bear a photograph of the principal.

- Verification of the address of the natural person:

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

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

Alternatively:

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

**Note:**

- Where "recent" means within the last three months.

- Verification of 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.

➢ Government issued personal identification number or other government issued unique identifier:

- The relevant government document

***The Company must collect relevant identification and verification of applicants who are legal persons/arrangements:***

➢ Legal Persons

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

➢ Verification of the existence of a legal person and identifying the principals thereof

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

- Take reasonable measures to understand the ownership and control structure of the applicant for business
- Verify and establish the existence of the legal person; and
- Determine the identity of the principals of the legal person.

In the case of a legal person, principals of applicants for business include the following:

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

- Company Directors

➢ In addition to the above, the Company must:

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

Where the underlying principals are <u>not</u> natural persons, the Company should establish the identity of the natural persons ultimately owning or controlling the business.

➢ <u>Private Companies</u>

- Obtaining an original or appropriately certified copy of the certificate of incorporation or registration;
- Checking with the relevant companies' registry that the company continues to exist;
- Reviewing a copy of the latest report and accounts if available (audited, where possible);
- Obtaining details of the registered office and place of business;
- Verifying the identity of the principals of the company as above;

➢ <u>Partnerships</u>

- Obtaining an original or certified copy of the partnership deed;
- Obtaining a copy of the latest reports and accounts;

- Verification of the nature of the business of the partnership to ensure that it is legitimate;
- Verifying the identity of the principals as above;

➢ Societes

- Obtaining an original or certified copy of an acte de société, in the case of Mauritian sociétés, checking with the Registrar of Companies that the société continues to exist;
- In the case of Mauritian sociétés, checking with the Registrar of Companies that the société is registered and continues to exist;
- In the case of foreign sociétés, obtaining a certificate of good standing in relation to them;
- Verifying the identity of the principals, administrators or gérants;

➢ Legal Arrangements

In this situation, trusts do not have separate legal personality, thus from business relationships through their business. It is the trustee of the trust who will enter a business relationship on behalf of the trust and should be considered along with the trust as the customer.

➢ Verification of the existence of a legal arrangement and identifying the principals

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

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

In the case of a legal arrangement, principals of applicants for business include the following:

- Settlors or Contributors of capital
- Trustees
- Beneficiaries

- Protectors
- Enforcers

The Company must:

- Verify the legal status of the legal arrangement;
- Identify and verify the identity of the principals of the applicant for business, that ism those natural persons with a controlling interest and those who comprise the mind and management of the legal arrangement; and
- Obtain information concerning the name of the trustee(s), its legal form, address and provisions binding the legal arrangement.

➢ Trust:

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

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

Additionally, where an applicant for business is a company, a trust, a partnership, a société or any other body of persons, the Company must verify the identity of the ultimate individual principals of such applicants in the same way that they are expected to verify the identity of customers who are natural persons.

### 7.5.2 Source of funds/property and source of wealth

In the identification of risk and prevention of money laundering, it is a pre-requisite for the Company to understand the origin or provenance of funds or property underlying a business relationship with a customer. All in all, by understanding the customer's source of funds/property and the customer's source of wealth is a crucial aspect of customer due diligence.

The Company shall distinguish the source of funds/property and the source of wealth. To clarify, the source of funds refers to the activity or transaction which generates the funds for a customer while the source of wealth refers to the activities which have generated the total net worth of the customer.

The Company uses a risk-based approach when determining whether to establish the proof of source of funds or the proof of source of wealth of a client. At all times, the Company does ensure that there is consistency between the information it holds on the Customer and the nature of transactions or proposed transactions.
The consistency between the provided information should be ensured by the Company. In case of any abnormality observed the Company must take additional measures to verify the information obtained. For example, the Company shall request for applicant's or a customer's source of wealth.

Source of Funds (**Annex VII**: List of Acceptable Documents for Proof of Source of Funds)

As defined by the FSC Handbook, the source of funds is the activity or transaction which generates the funds for a customer. As a requirement the Company ensures that it establishes the provenance of funds in the following cases:

- At the time of client onboarding, the source of funds of the client (UBO) is established;
- For any incoming funds e.g. funds coming in the client account, loan repayments, dividends, sale of shares;
- New investments in the client company; and
- Whenever there is third party funding involved.

Source of Wealth (**Annex VIII**: Specimen Template Letter for Source of Fund/Wealth)

The source of wealth relates to activities which have generated the total net worth of the customer. The establishment of the source of wealth is considered as one of the measures of enhanced due diligence that the Company applies in cases where there are high risk relationships.

### 7.5.3 Appropriate certification

In the case where an employee of a Company meets an applicant for business or the principals thereof face-to-face and has access to original verification of identity documentation, he or she may take copies of the verification of identity documentation and certify them personally as true copies of the original documentation.

In other cases, copies of the verification of identity documentation can be certified by a suitable person, such as a lawyer, notary, actuary, an accountant or any other person holding a recognized professional qualification, director or secretary of a regulated financial institution in Mauritius or in an equivalent jurisdiction, a member of the judiciary or a senior civil servant.

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

Moreover, in the case where certified copy documents are accepted, it is the Company's responsibility to ensure that the certifier is appropriate. In all cases, Company should also ensure that the customer's signature on the identification document matches the signature on the application form, mandate, or other document.

### 7.5.4 Omnibus Accounts

When establishing an omnibus account relationship with a regulated financial institution, the Company should undertake CDD measures on the applicant for business, that is, the regulated financial institution.

In addition to identifying and verifying the application for business, the Company must:

- Gather sufficient information regarding the applicant for business (the financial institution) to understand its business and to determine from publicly available information its professional reputation;
- Assess the adequacy of the financial institution's CDD process;
- Ascertain whether the financial institution has a physical presence in the jurisdiction in which it is incorporated. The Licensee must neither establish nor maintain an omnibus account for a financial

institution that has neither a physical presence in that jurisdiction nor is affiliated with a regulated financial group that has such a presence;

- Where the financial institution is a foreign entity, ensure that the country in which it is located is an equivalent jurisdiction with a view to determine whether the customer has been subject to sufficient CDD standards;
- Obtain approval of the Board of Directors before establishing new omnibus account relationships; and
- Document the respective responsibilities of each institution

### 7.5.5 Existing Customers

The Company must apply CDD requirements to existing customers on the basis of materiality and risk and conduct due diligence on such existing relationships when necessary.

In some situations as detailed below, it is desirable to conduct CDD checks on existing customers:

a) a transaction of significant amount takes place,
b) customer documentation standards change substantially,
c) there is a material change in the way the account is operated,
d) the Company becomes aware that it lacks sufficient CDD information about an existing customer.

### 7.5.6 High Risk Customers, Jurisdictions, Business Relationships and Enhanced Customer Identification

Enhanced due diligence measures

Enhanced due diligence would imply taking additional steps in relation to the identification and verification. This may include the following steps:

a) obtaining further customer due diligence information (identification and relationship information) from either the customer or independent sources (such as the internet, public or commercially available databases) including criminal records;

b) verifying additional aspects of the customer due diligence information obtained;
c) obtaining additional information required to understand the purpose and intended nature of such a business relationship;
d) taking appropriate and reasonable measures to establish the source of the funds and the wealth of the customer, any beneficial owner and underlying principal;
e) carrying out more frequent and more extensive ongoing monitoring on such business relationships with setting lower monitoring thresholds for transactions connected with such business relationships;
f) In case of individuals, bank statements for the last 6 months; and
g) Certificate of good standing, copy of latest audited financial statements for corporates.

Apart from the list provided above, the following documents may also be requested:

- Obtaining a professional and/or bank reference from a credible source.
- Obtaining a recent clearance certificate from authorities.

Upon the identification of such events, the CO shall seek to establish, as far as reasonably possible, that the risk aspect can be mitigated. In order to evaluate whether risk areas identified are genuine hits, additional documents may then be requested, on a case to case basis. Such documents will help to either gain the comfort that the client relationship may proceed or to interrupt the onboarding process and not commence any business relationship.

The Company applies the following enhanced due diligence measures, in addition to the CDD procedures as detailed above, under the following circumstances:

Politically Exposed Person (PEP)

The FIAMLR specifically provides for the definition of PEPs which includes:

"Domestic PEP" who is a natural person who is or has been entrusted domestically with prominent public functions in Mauritius and includes the Head of State and of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials and

such other person or category of persons as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

"Foreign PEPs" means a natural person who is or has been entrusted with prominent public functions by a foreign country, including Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials and such other person or category of persons as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

"International Organisation PEP" means a person who is or has been entrusted with a prominent function by an international organisation and includes members of senior management or individuals who have been entrusted with equivalent functions, including directors, deputy directors and members of the board or equivalent functions and such other person or category of persons as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

Enhanced CDD and enhanced ongoing monitoring (on a risk-sensitive basis) are required whenever a customer, or any beneficial owner of a customer, is or becomes a politically exposed person (PEP).

As part of the Company's duty to verify a customer's identification, the Company should gather sufficient information from a new customer, and check publicly available information, in order to establish whether or not the customer is a PEP or is an immediate family member or close associate of a PEP.

The Company shall investigate the source of funds before accepting a PEP or a close associate or immediate family member of a PEP.

The decision to establish a business relationship with a PEP is taken at senior management level.

For the identification of PEPs, the Company uses an automated electronic management information system, which belongs to an accredited third party provider, for undertaking among others CDD (e.g. Passport verification, PEP Research, Sanctions Lists, profile checks) on existing and prospective customers. The system

automatically identifies persons of interest, including but not limited to PEPs, Senior Government Officials, public figures or persons of influence, persons with potential red flags, such as a court cases or criminal re cords, sanctions etc. Additionally, the OGS (OnGoing Screening) feature on World Check is extensively used to continuously monitor clients (including all principles) in an automated way. Reports are generated automatically whenever there is a potential hit on any of the principles and risk assessment is updated respectively.

Additionally, the Company uses Google search engine to find the maximum amount of information which is publicly available on a client or entity. Word associations or combinations are used (such as [name of client] + scam, [name of client] + fraud etc.) during the Google verifications to ensure that a wide and broad research spectrum is allowed and covered. The results of such checks generally indicate whether there is any concern in relation to a client or whether that person should be categorized as a PEP.

The Company has:

- developed a clear policy on the acceptance of business relationships with such individuals. Prospective clients are screened out to determine whether they are PEP or not before accepting the client relationship. Whilst normal client relationships are subject to the standard CDD requirements, PEP relationships are escalated for approval by the CO;

- Register of PEP: All persons identified as PEPs, must be recorded in the PEP Register after having sought the relative approvals from senior management for acceptance of this category of clients. At the same time, Google Alerts are set to ensure that relevant team members are notified immediately in relation to any new article or matter of concern which may appear on Google. The Register is monitored by the CO and is reviewed on a monthly basis and fresh checks are conducted on a monthly basis as part of the monitoring process of PEPs;

- where applicants have been accepted and the said applicant or its beneficial owner is subsequently found to be, or subsequently becomes, a PEP, obtain the approval of senior management to continue such business relationships;

- obtain similar approval from senior management in cases of family members or close associates of PEPs;

- take enhanced due diligence measures to establish the source of funds and source of wealth of applicants, beneficial owners, family members or close associates of PEPs;
- conduct enhanced ongoing monitoring of the business relationships involving PEPs, family members or close associates of PEPs; and
- Training & Education: Staff members are the first line of defence in preventing and detecting money laundering and also have a crucial role to play in identifying clients or potential clients who are PEPs. It is therefore vital that the risk, policies, procedures and processes associated with such individuals are properly understood by relevant employees.

Close Family: Will include a PEP's direct family members including his/ her spouse, children, parents an d siblings. In any of these cases there may be circumstances which mitigate against such a categorisation including separation and estrangement although these facts should be investigated and recorded.

Close Associate: Will include a PEP's widely and publicly-known close business colleagues and/or personal advisors, in particular financial advisors or persons acting in a financial fiduciary capacity.

Non- face- to -face Customers

Where a Customer has not been physically present for identification process, the Company is obliged to apply equally effective customer due diligence and ongoing monitoring procedures for non-face-to-face customers and to put specific and adequate measures in place to mitigate this higher risk.

Based on their risk assessment, reporting entities should apply equally effective customer identification procedures and on-going monitoring standards for non-face-to-face customers as for those available for interview.

It is therefore important to undertake not only address verification but also to put in place additional procedures to establish personal verification. For example, there are three main areas of information (i.e. address details, employment details and the name and date of birth of the applicant), which could be checked to establish beyond reasonable doubt that a prospective new customer is genuine and that the named applicant is not the victim of an identity theft.

For non-face-to-face customers the Company:

- applies equally effective customer identification procedures for non-face-to-face customers as for those available for interview; and
- applies specific and adequate measures to mitigate the higher risk. Examples of measures to mitigate risk include:
    - Certification of documents presented;
    - Requisition of additional documents to complement those which are required for face-to-face customers;
    - Independent contact with the customer by the Company;
    - Seeks verification of the source of funds for the initial deposit, including sighting documentary evidence confirming the source of the funds.

Foreign customers from higher risk countries

The Financial Action Task Force's ("FATF") 40+9 Recommendations constitute the primary internationally recognised standards for the prevention and detection of money laundering and terrorist financing (http://www.fatf-gafi.org/countries/#high-risk).

The Company applies the following:

a. Exercises additional monitoring procedures and pays special attention to Business Relationships and transactions with persons, including companies and financial institutions, from countries which do not apply or apply inadequately the aforesaid recommendations.
b. Transactions with persons from the said countries, for which there is no apparent economic or visible lawful purpose, are further examined for the establishment of their economic, business or investment background and purpose. If the Company cannot be fully satisfied as to the legitimacy of a transaction, then a Suspicious Transaction Report is filed with FIU.

In order to implement the above, the Company takes into account:

a. the country assessment reports prepared by the FATF (http://www.fatf-gafi.org); and

b. the country assessment reports of other regional bodies like Asia/Pacific Group ,which Mauritius is a member, that have been established and work on the principles of FATF [e.g. the http://www.apgml.org/) and the International Monetary Fund (www.imf.org).

### 7.5.7 Declined Business

The Company does not accept business from the persons (list not exhaustive):

- Persons involved in Money Laundering and Terrorist Organisations
- Serving inmates
- Minors (under the age of 18 years old)
- Customers operating under false or misleading names that the Company become aware of who does not produce identity or verification within prescribed timeframe

### 7.5.8 Low Risk Relationships

Generally, the full range of CDD measures is applicable to all applicants for business. However, where the risk of money laundering or the financing of terrorism is lower and where information on the identity of the applicant for business is publicly available or where adequate checks and controls exist in national systems, it might be reasonable for the Company to apply simplified or reduced due diligence measures.

### 7.5.9 Simplified or reduced Due Diligence Measures

Simplified or reduced due diligence measures may be applied to the below listed bodies and the Company needs to obtain at a minimum the following information set out in the table below:

| If Applicant for business is | CDD Documentation required |
|---|---|
| A regulated financial services business based in Mauritius or in an equivalent jurisdiction, provided that the Company is satisfied that the applicant for business is not acting on behalf of underlying principals. | The Company must obtain and retain documentary evidence of the existence of the financial services business and of its regulated status. |

| | |
|---|---|
| A public company listed on the Stock Exchange of Mauritius or on Recognised, Designated and Approved Stock/ Investment Exchanges 16 or subsidiaries thereof.<br><br>Government administrations or enterprises and statutory bodies. | The Company must obtain a copy of the annual report and accounts of that public company and must verify that the individuals who purport to act on behalf of such entity have the necessary authority to do so.<br>The Company must also obtain and retain documentary evidence of the existence of the public company and of its listed status.<br>The Company must obtain and retain documentary evidence of identification and verification of identity. |
| A pension, superannuation or similar scheme which provides retirement benefits to employees where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme. | In all transactions undertaken on behalf of an employer-sponsored scheme, the Company must at a minimum identify and verify the identity of the employer and the trustees of the scheme. |

However, simplified CDD measures will not be acceptable whenever there is suspicion of money laundering or terrorist financing or specific higher risk scenarios apply.

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

- 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
- 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.

### 7.5.10 Termination of relationship

The Company shall terminate a business relationship where:

1) It is unable to comply with relevant CDD measures under applicable AML/CFT laws; and

2) It is unable to perform enhanced CDD as required under applicable AML/CFT laws.

The matter shall be escalated to senior management and the Company shall file a suspicious transaction report to the FIU.

### 7.5.11 Targeted Financial Sanctions

The Company applies risk-based sanctions screening against United Nations Security Council Consolidated List and Mauritius targeted financial sanctions lists (the "Sanctions Lists"). This involves the screening of all relevant information related to customers, potential customers, associated parties, beneficial owners, PEPs, transactions and business activities against the Sanctions Lists to determine if any person are designated persons under the Sanctions Lists to ensuring compliance with applicable laws.

The Company ensures that the screening controls are applied prospectively prior to engaging in a relationship or a transaction and that any potential sanctions-related alerts and concerns identified through application of those controls are resolved prior to completing the engagement or transaction.

Screening is done through a recognised automated electronic management information system as well as open source data screening such as Google Checks for Judgements, Litigations, Money Laundering or Terrorist Financing. If a positive designated person match is confirmed, the Company shall immediately, meaning no later than 24 hours, freeze the asset(s) of the said designated person(s) and report promptly to the National Sanctions Secretariat in Mauritius. Clients are screened depending on the level of risk on a periodic basis to identify clients or beneficial owners who may have become designated persons since being onboarded. High risk relationships are screened every year against Sanctions Lists while Medium risk are screened every 2 years and Low risk every 3 years. PEP clients are screened on an ongoing basis with Google Alert and OGS (On-going Screening) feature on World Check and controls are resolved prior to completing the engagement or transaction. The Company shall keep records of designated person screening, positive hits, false positives and negatives results.

## 8 RECORD KEEPING

The Company should arrange for records to be kept of all transactions in accordance to the below. The Company must keep the records for a period of seven (7) years after the completion of the transaction.

More specifically, the books and records shall include:

a) all records obtained through CDD measures, including account files, business correspondence and copies of all documents evidencing the identity of customer and beneficial owners, and records and the results of any analysis undertaken in accordance with the Act, all of which shall be maintained for a period of not less than seven (7) years after the business relationship has ended;
b) records for both domestic and international transactions, that are sufficient to permit reconstruction of each individual transaction for both account holders and non-account holders, which shall be maintained for a period of seven (7) years after the completion of the transaction; and
c) copies of all suspicious transaction reports made or other reports made to FIU in accordance with the Act, including any accompanying documentation, which shall be maintained for a period of at least seven (7) years from the date the report was made.

Records of CDD procedures

The first category of records that must be maintained is records of all CDD measures applied in respect of the customers.

All applications and documents produced to verify identity must be kept for the duration of each relationship and for the stipulated period thereafter.

The following information should be included:

a) copies of the identification data obtained to verify the identity of all customers, beneficial owners and underlying principals;

b) copies of any customer files, account files, business correspondence and information relating to the business relationship; or

c) information as to where copies of the identification data and other files may be obtained.

Transaction and correspondence records

The second category of records that must be maintained is records of all transactions and related correspondence carried out by the Company.

All transactional records should be retained for the stipulated period after the completion of the transaction to which they relate.

Where applicable, transaction records must adequately identify:

a. the name and address of the customer, beneficial owner and underlying principal;
b. if a monetary transaction, the currency and amount of the transaction;
c. account name and number or other information by which it can be identified;
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.

For Internal and external suspicious reports filed, the Company is required to maintain the following records:

a. the internal suspicion reports received by the MLRO;
b. records of actions taken under the internal and external reporting requirements;
c. when the MLRO has considered information or other material concerning the reports, but has not made a disclosure of suspicion to the FIU, a record of the information or material that was considered and the reason for the decision; and
d. all reports made by the MLRO to the FIU.

Training records

The Company must maintain records of all AML/CFT training delivered to the employees. Especially, records should include:

a. the dates AML/CFT training was provided;
b. the nature of the training, including details of contents and mode of delivery; and
c. the names of the employees who received training.

Compliance monitoring records

Records must be kept at all levels of the Company's compliance, to ensure that appropriate policies, procedures and controls are in place and are being properly adhered to.

Those records must include the following:

a. reports by the MLRO to the Board and management;
b. records of consideration of those reports and of any action taken as a consequence; and
c. any records made within the Company or by other parties in respect of compliance of the Company with the relevant AML/CFT laws and guidelines.

**Note:**

- Customer transaction records must provide a clear and complete transaction history of incoming and outgoing funds or assets.
- The Company must maintain records of all transactions undertaken on behalf of the customer during the course of a business relationship, either in the form of original documents or copies. Where copies of the original identification documents (passports, national ID, drivers licence or any acceptable form of identification) are maintained, these copies should be duly certified in accordance with the CDD measures in place.

## 9 EMPLOYEES' SCREENING, EDUCATION AND TRAINING

### Employees screening

Under Section 22(1)(b) of Regulations, the Company shall implement programmes for screening procedures so that high standards are maintained when hiring employees. Furthermore, 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 Company, to maintain awareness of the laws and regulations relating to money laundering and terrorism financing to:

a. assist them in recognising transactions and actions that may be linked to money laundering or terrorism financing; and
b. instruct them in the procedures to be followed where any links have been identified as per above.

### Board of Directors oversight

The Board must be aware of the obligations of the Company in relation to employee screening and training. The Company must ensure that the training provided to officers and employees is comprehensive and ongoing and that the officers and employees are aware of ML and TF, the associated risks and vulnerabilities of the Company, and their corresponding obligations.

The Board should ensure that it is provided with adequate information on a sufficiently regular basis in order to satisfy itself that the Company's employees are suitably trained to fulfil their personal and corporate responsibilities.

### Screening Requirements

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

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

c. obtaining and confirming details of any regulatory action or action by a professional body taken against the prospective employee;
d. obtaining and confirming details of any criminal convictions, including the provision of a check of the prospective employee's criminal record; and
e. screening the employees against the UN's list of designated persons under terrorist and proliferation financing targeted financial sanctions The financial institution should also carry out periodic ongoing of its employees against the UN's list of designated persons under terrorist and proliferation financing targeted financial sanctions.

**Training Methods and Frequency of Training**

While there is no single or definitive way to conduct training, the critical requirement is that training is adequate and relevant to those being trained and that the content of the training reflects good practice.

The guiding principle of all AML and CFT training should be to encourage directors, officers and employees, irrespective of their level of seniority, to understand and accept their responsibility to contribute to the protection of the financial institution against the risks of ML and TF.

Training should highlight to directors, officers and employees the importance of the contribution that they can individually make to the prevention and detection of ML and TF.

The Company must provide basic AML/CFT training to all employees at least every year. Some categories of employees should receive additional, specialized training according to their roles.

Training will also need to be carried out more frequently to meet the requirements of the Regulations if new legislation or significant changes are introduced, or where there have been significant technological developments within the Company or with the introduction of new products, services or practices.

**Content of Training**

In providing the training required, pursuant to Section 22(1)(c) of the Regulations the Company must:

a. provide appropriate training to directors, officers and employees to enable them to competently analyse information and documentation, so as to enable them to form an opinion on whether the transactions and actions may be linked to money laundering or terrorism financing;
b. detail procedures that need to be followed if any links to money laundering or terrorism financing have been identified;
c. prepare and provide to employees a copy, in any format, of the financial institution's policies, procedures and controls manual for AML and CFT; and
d. ensure employees are fully aware of all applicable legislative requirements.

The ongoing training shall cover:

a. the Act, the Regulations as well as the AML/CFT Handbook;
b. the implications of non-compliance by employees to requirements; and
c. the Company's policies, procedures and controls for the purposes of foreseeing, preventing and detecting ML and TF.

The financial institution must ensure that the ongoing training provided to directors, officers and employees also covers, to a minimum (not exhaustive):

a. the requirements for the internal and external disclosing of suspicion;
b. the criminal and regulatory sanctions in place, both in respect of the liability of the financial institution and personal liability for individuals, for failing to report information in accordance with the policies, procedures and controls of the financial institution;
c. the identity and responsibilities of the MLRO, CO and Deputy MLRO;
d. dealing with business relationships or occasional transactions subject to an internal disclosure, including managing the risk of tipping off and handling questions from customers;
e. those aspects of the financial institution's business deemed to pose the greatest ML and TF risks, together with the principal vulnerabilities of the products and services offered by the financial institution, including any new products, services or delivery channels and any technological developments;

f. new developments in ML and TF, including information on current techniques, methods, trends and typologies;

g. the Company's policies, procedures and controls surrounding risk and risk awareness, particularly in relation to the application of CDD measures and the management of high risk and existing business relationships;

h. the identification and examination of unusual transactions or activity outside of that expected for a customer;

i. the nature of terrorism funding and terrorist activity in order that employees are alert to transactions or activity that might be terrorist-related;

j. the vulnerabilities of the financial institution to financial misuse by PEPs, including the effective identification of PEPs and the understanding, assessing and handling of the potential risks associated with PEPs; and

k. UN, EU and other sanctions and the financial institution's controls to identify and handle natural persons, legal persons and other entities subject to sanction.

**Training of the Board and Management**

The Board and Management must receive adequate training to ensure they have the knowledge to assess the adequacy and effectiveness of policies, procedures and controls to counter the risk of ML and TF.

The additional training provided to the Board and Management must include, at least, a clear explanation and understanding of:

- offences and penalties arising for non-reporting or for assisting money launderers or those involved in terrorist financing;
- requirements for CDD including verification of identity and retention of records; and
- in particular, the application of the financial institution's risk-based strategy and procedures.

**The Money Laundering Reporting Officer and Deputy Money Laundering Reporting Officer**

As MLROs and Deputy MLROs have significant responsibility for the receipt, evaluation and where appropriate external reporting of suspicious transactions to the FIU, should be given additional training.

The additional training must be in-depth and specific with regard to:

a. AML/CFT legislative and regulatory requirements;
b. the international standards and requirements on which the Mauritius' strategy is based, namely the FATF 40 Recommendations and ML/TF typology reports that are relevant to their business;
c. the identification and management of ML/TF risk;
d. the design and implementation of internal systems of AML/CFT control;
e. the design and implementation of AML/CFT compliance testing and monitoring programs;
f. the identification and handling of suspicious activity and arrangements and suspicious attempted activity and arrangements;
g. the money laundering and terrorist financing vulnerabilities of relevant services and products;
h. the handling and validation of internal disclosures;
i. the process of submitting an external disclosure;
j. liaising with law enforcement agencies;
k. money laundering and terrorist financing trends and typologies; and
l. managing the risk of tipping off.

**The Compliance Officer**

The CO is responsible for ensuring continued compliance with the requirements of the Act and Regulations and having an overall oversight of the program for combatting money laundering and terrorism financing and other illegal activities.

The CO should receive 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 controls in place to prevent and detect ML and TF.

In line with the Competency Standards issued by the FSC, the Compliance Officer, MLRO and DMLRO need to complete at least 10 CPD points of AML.CFT related training.

## 10 REPORTING TO THE FIU

### Suspicious Transactions and Activities

A suspicious transaction has been defined as a transaction which:

a. gives rise to a reasonable suspicion that it may involve:
    i. the laundering of money or the proceeds of any crime; or
    ii. funds linked or related to, or to be used for, terrorist financing or by prescribed organisations, whether or not the funds represent the proceeds of a crime;
b. is made in circumstances of unusual or unjustified complexity;
c. appears to have no economic justification or lawful objective;
d. is made by or on behalf of a person whose identity has not been established to the satisfaction of the person with whom the transaction is made; or
e. gives rise to suspicion for any other reason.

The employees who determine an unusual transaction or attempted transaction have to report it promptly to the Money Laundering Reporting Officer and must not proceed further with the transaction unless the Money Laundering Reporting Officer has given approval.

*A Suspicious activity* refers to a series of suspicious acts or transactions which are conducted over time and form a pattern or trend. When the employees identify a suspicious activity or attempted activity need to report it promptly to the Money Laundering Reporting Officer and must not proceed further with the activity/transaction unless the Money Laundering Reporting Officer has given approval.

Where the Company identifies any unusual activity in the course of a business relationship or occasional transaction the Company should:

a. perform appropriate scrutiny of the activity;
b. obtain EDD only if this will not tip off the client; and
c. consider whether to make an internal disclosure in accordance with the reporting procedures.

Unusual activity includes, but not limited to, any activity or information relating to a business relationship, occasional transaction or an attempted transaction where there is no apparent economic or lawful purpose, including transactions that are complex; both large and unusual; or of an unusual pattern.

The employees must not inform the customer that the transaction or attempted transaction is unusual or when an activity is suspicious but must refer these cases to the CO.

Examples of suspicious transactions can be found in **Annex III** and of suspicious activities can be found in **Annex IV.**

**Reporting process**

The Company's employees will discharge their obligation under the Act by disclosing their suspicions to the MLRO in accordance with the Company's internal procedures.

At the time that the MLRO validates an internal suspicious transaction report, he/she must report it and the circumstance surrounding it as soon as possible as practicable but not later than 5 working days from the day on which it becomes aware of a transaction to the FIU by using the form prescribed by the FIU.

A sample Internal Disclosure Form to the MLRO is found at **Annex V**).

The MLRO, may consider the following when investigating a transaction or an application:

- Is the size of the transaction consistent with the usual transactions of the Customer?
- Does the transaction make sense in the context of who the Customer is and what they do for a living?
- Has the pattern of transactions done by this Customer changed?

- Where the transaction involves overseas payments, is there a sensible reason why the Customer is engaging in the transaction?

When the MLRO decides that something is not suspicious, he should record his reasons in the file.

All the suspicious transactions should be reported to the FIU as soon as practicable but not later than five (5) working days after establishing suspicion. A suspicious transaction report (STR) shall be submitted to the FIU electronically using GOAML.

The **electronic submission** of STRs can be done in the following two manners:

a) In XML format; or
b) By completing an online web-based STR form

both options of STR submission are done via the FIU website.

**Registration for online submission**

To be able to submit STRs via the FIU website, the MLRO must be registered with the FIU. Once the reporting entity has been registered, verified and accepted by the FIU, the MLRO can submit STRs online.

**Large Cash Transactions**

The Company shall report to the FIU the prescribed particulars of any transaction in excess of the MUR 500,000 and its equivalent.

When two or more transactions totalling MUR 500,000 or the equivalent amount in foreign currency are conducted on behalf of the same individual within a short lapse of time, and the reporting entity or person is required to keep a cash transaction record knows that these transactions or transfers are conducted by, or on behalf of, the same person or entity, they must be treated as a single transaction and reported to the FIU, unless they are exempted.

**Electronic funds transfers (EFTs)**

Where the Company sends money through electronic transfer in excess of the prescribed amount out of Mauritius or he receives money in excess of the prescribed amount from outside Mauritius on behalf, or on the instruction of, another person, he shall, within the prescribed period after the money was transferred, report the transfer, together with the prescribed particulars, to FIU.

The MLRO shall keep a register of suspicious transaction reports, recording the date it was lodged and other identifying information. This register shall be stored securely so no other employee can access it.

**Tipping off**

Once an internal suspicion report to a MLRO or a suspicious transaction report has been submitted to the FIU, it is an offence when a person 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 Company must ensure that due care is taken during subsequent enquiries so as not to alert the customer about the disclosure.

Moreover, under section 16 of the Act no person directly or indirectly involved in the reporting of a su spicious transaction is allowed to inform any person involved in the transaction or an unauthorized third party that the transaction has been reported or that information has been supplied to the FIU on request.

Further, under Section 16 of FIAMLA 2002, ***'tipping off'*** the customer or any other person is a criminal offence and upon conviction, a fine not exceeding 5 million rupees and imprisonment not exceeding 10 years are the prescribed penalties.

## 11 INDEPENDENT AUDIT

### INDEPENDENT AUDIT ON AML/CFT

In line with Regulation 22 (1) (d) of the FIAML Regulations 2018 and the guidance under Chapter 13 of the Handbook the Company will appoint an external independent service provider to conduct an independent audit to:

1) examine and evaluate the adequacy and effectiveness of the policies, controls and procedures adopted by the Company to comply with the requirements of the FIAMLA and FIAML Regulations 2018;

2) make recommendations in relation to those policies, controls and procedures; and

3) monitor the Company's compliance with those recommendations.

The independent firm shall be provided access to all records of the Company to enable them to conduct the audit.

The Company shall consider the recommendations and observations of the independent audit report to address any element of non-compliance or improvement of its system and procedures. The Company shall also ensure that appropriate follow-ups are undertaken vis-à-vis the recommendations and observations made by the independent audit function.

The frequency at which the independent audit will be conducted will be determined by the Board taking into consideration all relevant factors.

The independent audit exercise should be risk-based. The independent audit exercise should mandatorily test compliance in the following non-exhaustive areas:

- AML/CFT policies and procedures;
- Internal Risk Assessment;
- Risk Assessment on the use of third-party service providers (Outsourcing);
- Compliance Officer function and effectiveness;
- MLRO function and effectiveness;

- Implementation and Effectiveness of Mitigating Controls, including customer due diligence and enhanced measures;
- AML/CFT Training;
- Record Keeping Obligations;
- Targeted Financial Sanctions; and
- Suspicious Transaction Monitoring and Reporting.

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

The audit process to be carried out independently. This implies that the person or firm conducting the audit should be independent and must not be involved in the development of the Company's AML/CFT risk assessment, or the establishment, implementation or maintenance of its AML/CFT programme.

The Company shall take great care in choosing the resource to carry out the audit with particular emphasis on the necessary skills, qualifications, relevant experience of the audit process and a proper understanding of the applicable laws and regulations.

The independent audit report must express views on whether the AML/CFT risk assessment and the AML/CFT programme comply with the requirements of FIAMLA and supporting legislations and whether the programme is functioning effectively in practice as required and intended, and has been over the course of the period.

The independent audit will involve obtaining a good understanding of the Company's business, reviewing relevant core documents, file testing, testing of the live application of policies and procedures, and interviewing a cross-section of players. The audit process must have sufficient depth and breadth to support the findings and to make the report worthwhile.

Within the framework of the AML/CFT programme itself, the independent audit shall inter alia:

- address the adequacy of AML/CFT risk assessment, including whether it addresses the specific business activities of that particular financial institution;

- test compliance of the financial institutions' AML/CFT programme, policies and procedures with the FIAMLA, FIAML Regulations 2018, and the AML/CFT Handbook and a general review of the effectiveness of the compliance function considering the risks identified through the risk assessment;

- assess the employees' adherence to the AML policies and procedures;

- assess employees' knowledge of the AML/CFT laws, regulations, guidance, and policies & procedures;

- examine the adequacy of Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) policies, procedures and processes, and whether they comply with higher-level internal requirements in the financial institution. This may include considering the adequacy of onboarding paperwork and considering the adequacy of enhanced measures against the findings of the risk assessment;

- conduct appropriate customer file testing, with particular emphasis on high risk operations (products, service, customer and geographical locations);

- examine the adequacy of the policies and procedures as well as the processes for identifying and reporting suspicious transactions promptly;

- if an automated system is not used to identify or aggregate large transactions, the audit should include sample test of how the compliance officer conducts monitoring;

- conduct appropriate transaction file testing, including a review of 'not filed' (closed as not suspicious) internal suspicious transactions reports, to determine the adequacy, completeness and effectiveness of the STR filing process;

- examine the adequacy of the policies and procedures as well as the processes for screening for targeted financial sanctions as well as implementing prohibitions, freezing assets, and reporting to competent authorities;

- review how the financial institution is screening for targeted financial sanctions without delay when onboarding clients or conducting transactions and when the lists are updated (within hours), and the appropriateness of periodic screening frequency;

- conduct appropriate testing of TFS screening records, including a review of false positives, to determine the adequacy, completeness and effectiveness of the TFS process;

- examine the integrity and the accuracy of the management information systems use in the AML compliance programme; and

- assess training adequacy including its comprehensiveness, accuracy of materials, training schedule and attendance tracking.

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

- covers all relevant components of the compliance programme as required under FIAMLA and relevant regulations;

- was adequate and effective throughout a specified period;

- identifies areas where the Company did not meet minimum legal or regulatory standards, and include actions that are required to rectify non-compliance as well as identifying areas for recommended changes in behaviour and practice to improve the effectiveness of the AML/CFT programme's implementation. This includes an indication of where there are potential failings and a recommended course of action.

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

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

The independent audit report shall be filed with the FSC upon the latter's request.

## ANNEX I

**Customer Risk Factors**

When identifying the risk associated with its customers, including the beneficial owners of customers, the financial institution shall consider the risk related to:

(a) the customer's (and beneficial owner's) business or professional activity;
(b) the customer's (and beneficial owner's) reputation; and
(c) the customer's (and beneficial owner's) nature and behaviour.

- Risk factors that may be relevant when considering the risk associated with a customer's or beneficial owner's business or professional activity may include:

(a) Does the customer or beneficial owner have links to sectors that are commonly associated with higher corruption risk, such as construction, pharmaceuticals and healthcare, the extractive industries or public procurement?
(b) Does the customer or beneficial owner have links to sectors that are associated with higher ML and/or TF risk, for example, certain money service providers ("MSPs"), casinos or dealers in precious metals?
(c) Does the customer or beneficial owner have links to sectors that involve significant amounts of cash?
(d) Where the customer is a legal person or legal arrangement, what is the purpose of their establishment? For example, what is the nature of their business?
(e) Does the customer have political connections, for example, are they a PEP, or is the beneficial owner a PEP? Does the customer or beneficial owner have any other relevant links to a PEP, for example, are any of the customer's directors PEPs and, if so, do these PEPs exercise significant control over the customer or beneficial owner? In line with Regulation 12(1) of FIAML Regulations 2018, where a customer or the applicant for business is a PEP, the financial institution shall apply EDD measures.
(f) Does the customer or beneficial owner hold another prominent position or enjoy a high public profile that might enable them to abuse this position for private gain? For example, are they senior local or regional public officials with the ability to influence the awarding of public contracts, decision-making

members of high-profile sporting Boardies or individuals who are known to influence the government and other senior decision-makers?

(g) Is the customer a legal person subject to enforceable disclosure requirements that ensure reliable information about the customer's beneficial owner is publicly available, for example, public companies listed on stock exchanges that make such disclosure a condition for listing?

(h) Is there evidence that the customer has been subject to supervisory sanctions or enforcement for failure to comply with AML and CFT obligations or wider conduct requirements in recent years?

(i) Is the customer a public administration or enterprise from a country or territory with high levels of corruption?

(j) Is the customer's or the beneficial owner's background consistent with what the firm knows about their former, current or planned business activity, their business's turnover, the source of funds and the customer's or beneficial owner's source of wealth?

- The following risk factors may be relevant when considering the risk associated with a customer's or beneficial owner's reputation:

(a) Are there adverse media reports or other relevant sources of information about the customer, for example, are there any allegations of criminality or terrorism against the customer or the beneficial owner? If so, are these reliable and credible? The financial institution should determine the credibility of allegations on the basis of the quality and independence of the source of the data and the persistence of reporting of these allegations, among other considerations.

(b) Has the customer, beneficial owner or anyone publicly known to be closely associated with them, had their assets frozen due to administrative or criminal proceedings or allegations of terrorism or TF? Does the firm have reasonable grounds to suspect that the customer or beneficial owner or anyone publicly known to be closely associated with them has, at some point in the past, been subject to such an asset freeze?

(c) Does the firm know if the customer or beneficial owner has been the subject of an internal or external disclosure in the past?

(d) Does the firm have any in-house information about the customer's or the beneficial owner's integrity, obtained, for example, in the course of a long-standing business relationship?

- The following risk factors may be relevant when considering the risk associated with a customer's or beneficial owner's nature and behaviour. The financial institution should note that not all of these risk factors will be apparent at the outset, they may emerge only once a business relationship has been established:

(a) Does the financial institution have any doubts about the veracity or accuracy of the customer's or beneficial owner's identity?

(b) Are there indications that the customer might seek to avoid the establishment of a business relationship? For example, does the customer look to carry out one transaction or several one-off transactions where the establishment of a business relationship might make more economic sense?

(c) Is the customer's ownership and control structure transparent and does it make sense? If the customer's ownership and control structure is complex or opaque, is there an obvious commercial or lawful rationale?

(d) Do the customer issue bearer shares or does it have nominee shareholders?

(e) Is the customer a legal person or legal arrangement that could be used as a personal asset holding vehicle?

(f) Is there a sound reason for changes in the customer's ownership and control structure?

(g) Do the customer request transactions that are complex, unusual or unexpectedly large or have an unusual or unexpected pattern without an apparent economic or lawful purpose or a sound commercial rationale? Are there grounds to suspect that the customer is trying to evade specific thresholds, such as those subject to mandatory reporting, either in Mauritius or the customer's home country or territory?

(h) Does the customer request unnecessary or unreasonable levels of secrecy? For example, is the customer reluctant to share identification data, or do they appear to want to disguise the true nature of their business?

(i) Can the customer's or beneficial owner's source of funds or source of wealth be easily established, for example, through their occupation, inheritance or investments?

(j) Does the customer use the products and services they have taken out as expected when the business relationship was first established?

(k) Is the customer an NPO whose activities could be abused for TF purposes?

**Countries and Territories Risk Factors**

When identifying the risk associated with countries and territories, the financial institution can consider the risk related to those countries and territories with which the customer or beneficial owner has a relevant connection. Additionally, the following can be considered:

The financial institution should note that the nature and purpose of the business relationship will often determine the relative importance of individual country and geographical risk factors.

For example:

(a) Where the funds used in the business relationship or occasional transaction have been generated abroad, the level of predicate offences to ML and the effectiveness of a country's or territory's legal system will be particularly relevant.

(b) Where funds are received from, or sent to, countries or territories where groups committing terrorist offences are known to be operating, the financial institution should consider to what extent this could be expected to, or might give rise to, suspicion based on what the financial institution knows about the purpose and nature of the business relationship or occasional transaction.

(c) Where the customer or beneficial owner is a legal person or legal arrangement, the firm should take into account the extent to which the country or territory in which the customer or beneficial owner is registered effectively complies with international tax transparency standards.

- Risk factors that the financial institution can consider when identifying a country's or territory's level of transparency and tax compliance include:

(a) Is there information from more than one credible and reliable source that the country has been deemed compliant with international tax transparency and information sharing standards? Is there evidence that relevant rules are effectively implemented in practice?

Examples of possible sources include reports by the Global Forum on Transparency and the Exchange of Information for Tax Purposes of the OECD, which rate jurisdictions for tax transparency and information sharing purposes; assessments of the country's or territory's commitment to automatic

exchange of information based on the Common Reporting Standard; assessments of compliance with Recommendations 9, 24 and 25 and Immediate Outcomes 2 and 5 of the FATF Recommendations by the FATF or FATF-style regional Boardies; and IMF assessments (for example, IMF staff assessments of offshore financial centres).

(b) Has the country or territory committed to, and effectively implemented, the Common Reporting Standard on Automatic Exchange of Information, which the G20 adopted in 2014?

(c) Has the country or territory put in place reliable and accessible beneficial ownership registers?

- Risk factors that may be relevant when considering the risk associated with a product service or transaction's complexity include:

(a) To what extent do products or services allow the customer or beneficial owner structures to remain anonymous, or facilitate hiding their identity? Examples of such products and services include bearer shares, fiduciary deposits, personal asset holding vehicles, and legal entities such as foundations that can be structured in such a way as to take advantage of anonymity and allow dealings with shell companies or companies with nominee shareholders.

(b) To what extent is it possible for a third party that is not part of the business relationship to give instructions, for example, in the case of certain correspondent banking relationships?

- Risk factors that may be relevant when considering the risk associated with a product, service or transaction's complexity include:

(a) To what extent is the transaction complex and does it involve multiple parties or multiple countries or territories, for example, in the case of certain trade finance transactions? Are transactions straightforward, for example, are regular payments made into a pension fund?

(b) To what extent do products or services allow payments from third parties or accept overpayments where this would not normally be expected? Where third party payments are expected, does the firm know the third party's identity, for example, is it a state benefit authority or a guarantor?

(c) Does the financial institution understand the risks associated with its new or innovative product or service, in particular where this involves the use of new technologies or payment methods?

- Risk factors that may be relevant when considering the risk associated with a product service or transaction's value or size include:

(a) To what extend are products or services cash intensive, for example, many payment services and certain current accounts?

(b) To what extend do products or services facilitates or encourage high-value transactions?

(c) Are there any caps on transaction values or levels of premium that could limit the use of the product or service for ML and TF purpose?

## ANNEX II

**List of non-cooperative countries and territories and countries with deficiencies in their AML/CFT regime**

### NON-COOPERATIVE COUNTRIES AND TERRITORIES

The FATF recommends that special attention should be given to business relations and transactions with persons, including companies and financial institutions, from the non-cooperative countries and territories (NCCT).

The Company is required to check the FATF website (http://www.fatf-gafi.org/countries/#high-risk) for regular updates on the above countries.

## ANNEX III

**The following are examples of common indicators that may point to suspicious or unusual transactions:**

- Client admits or makes statements about involvement in criminal activities;
- Client does not want correspondence sent to home address;
- Client appears to have accounts with several financial institutions in one area for no apparent reason;
- Client conducts transactions at different physical locations in an apparent attempt to avoid detection;
- Client repeatedly uses an address but frequently changes the names involved;
- Client is accompanied and watched at all relevant times;
- Client shows uncommon curiosity about internal systems, controls and policies;
- Client has only vague knowledge of the amount of a deposit;
- Client presents confusing details about the transaction or knows few details about its purpose;
- Client appears to informally record large volume transactions, using unconventional bookkeeping methods or "off-the-record" books;
- Client over justifies or explains the transaction;
- Client is secretive and reluctant to meet in person;
- Client is nervous, not in touch with the transaction;
- Client is involved in transactions that are suspicious but seems blind to being involved in money laundering activities;
- Client's home or business telephone number has been disconnected or there is no such number when an attempt is made to contact client shortly after opening account;
- Normal attempts to verify the background of a new or prospective client are difficult;
- Client appears to be acting on behalf of a third party, but does not tell you;
- Client is involved in activity out-of-keeping for that individual or business;
- Client insists that a transaction be done quickly;
- Inconsistencies appear in the client's presentation of the transaction;

- The transaction does not appear to make sense or is out of keeping with usual or expected activity for the client;
- Client appears to have recently established a series of new relationships with different financial entities;
- Client attempts to develop close rapport with staff;
- Client uses aliases and a variety of similar but different addresses;
- Client spells his or her name differently from one transaction to another; or
- Client provides false information or information that you believe is unreliable..

## ANNEX IV

**The following are examples of suspicious activity:**

- Accounts are used to receive or disburse large sums but show virtually no normal business related activities, such as the payment of salaries, invoices, etc.;
- Accounts have a large volume of deposits in bank drafts, cashier's cheques;
- Money orders or electronic funds transfers, which is inconsistent with the client's business;
- Accounts have deposits in combinations of monetary instruments that are atypical of legitimate business activity (for example, deposits that include a mix of business, payroll, and social security cheques);
- Accounts have deposits in combinations of cash and monetary instruments not normally associated with business activity;
- Business does not want to provide complete information regarding its activities;
- Financial statements of the business differ noticeably from those of similar businesses;
- Representatives of the business avoid contact with the branch as much as possible, even when it would be more convenient for them;
- Deposits to or withdrawals from a corporate account are primarily in cash rather than in the form of debit and credit normally associated with commercial operations;
- Client maintains a number of trustee or client accounts that are not consistent with that type of business or not in keeping with normal industry practices;
- Client operates a retail business providing cheque-cashing services but does not make large withdrawals of cash against cheques deposited;
- Client pays in cash or deposits cash to cover bank drafts, money transfers or other negotiable and marketable money instruments;
- Client purchases cashier's cheques and money orders with large amounts of cash;
- Client deposits large amounts of currency wrapped in currency straps;
- Client makes a large volume of seemingly unrelated deposits to several accounts and frequently transfers a major portion of the balances to a single account at the same bank or elsewhere;

- Client makes a large volume of cash deposits from a business that is not normally cash intensive;
- Client makes large cash withdrawals from a business account not normally associated with cash transactions;
- Client consistently makes immediate large withdrawals from an account that has just received a large and unexpected credit from abroad;
- Client makes a single and substantial cash deposit composed of many large bills;
- Small, one-location business makes deposits on the same day at different branches across a broad geographic area that does not appear practical for the business;
- There is a substantial increase in deposits of cash or negotiable instruments by a company offering professional advisory services, especially if the deposits are promptly transferred;
- There is a sudden change in cash transactions or patterns;
- Client wishes to have credit and debit cards sent to international or domestic destinations other than his or her place of business;
- There is a marked increase in transaction volume on an account with significant changes in an account balance that is inconsistent with or not in keeping with normal business practices of the client's account;
- Asset acquisition is accompanied by security arrangements that are not consistent with normal practice;
- Unexplained transactions are repeated between personal and commercial accounts;
- Activity is inconsistent with stated business;
- Account has close connections with other business accounts without any apparent reason for the connection;
- Activity suggests that transactions may offend securities regulations or the business prospectus is not within the requirements; or
- A large number of incoming and outgoing wire/electronic transfers take place for which there appears to be no logical business or other economic purpose, particularly when this is through or from locations of concern, such as countries known or suspected to facilitate money laundering activities.

**ANNEX V**

**Sample Internal Disclosure Form to MLRO**

**1. Reporting Employee**

Name :_____

Telephone No : _____

**2. Client**

Client Name :_____

Address :_____

Contact Name :_____

Contact Telephone No : _____

Date Client Relationship

Commenced :_____

Client reference : _____

**3. Information/Suspicion**

Suspected Information/

Transaction :_____

Reasons for Suspicion:

_____

Please attach copies of any relevant documentation to this report.

**Reporter's Signature:**_____ Date: _____

**It is an offence to advise the customer/client or anyone else of your suspicion and report.**

**This report will be treated in the strictest confidence.**

MLRO Use:

Date received.....Time received: ..... Ref.....

FIU advised: Yes/No…. Date: ……. Ref…….

## ANNEX VII

## LIST OF ACCEPTABLE DOCUMENTS FOR PROOF OF SOURCE OF FUNDS

| Potential Scenario | Examples of acceptable Proof of source of funds |
|---|---|
| • **Person is in employment** | 3 months bank statement showing salary being credited |
| • **In case of inheritance** | Letter from notary confirming inheritance and amount inherited |
| • **Business profits** | Financial statements of the company |
| • **If person is a consultant or contractual employment** | The valid contract of employment |
| • **In case of savings** | 3 months bank statements showing the relevant amount |
| • **Sale of property** | letter from notary confirming the sale and the value that the property was sold |
| • **In case of insurance benefit** | Letter from insurance company relating to the benefit |

**ANNEX VIII**

**TEMPLATE LETTER FOR THE ESTABLISHMENT OF SOURCE OF FUNDS AND SOURCE OF WEALTH**

Dated this _____

**To:**

Dear Sir,

**Attestation for Source of Income & Source of Wealth for _____**

I confirm having known Mr./Mrs./Ms._____for_____years in my capacity as personal (accountant/lawyer etc.). I know Mr./Mrs./Ms._____to be a person of integrity and honest dealing.

I confirm the following based on my professional experience and relationship with Mr./Mrs./Ms._____:

1. **Source of Income:**

   Mr./Mrs./Ms_____is currently employed at_____and derives a monthly salary in his capacity as Director/Shareholder of (Company name(s)) since (year).

2. **Source of Wealth:**

   i. Mr./Mrs./Ms._____net worth has been accumulated over (amount of years) being in employment in various companies as follows:

      (Name of companies): (position)

      (Name of companies): (position)

   ii. Mr./Mrs./Ms._____also derives dividends from various companies in which he/she has interest as shareholder and/or beneficial owner. The companies are: (Name of Company).

iii. Mr./Mrs./Ms._____has also inherited property from his/her deceased relatives in (year), inheritance consisting of (immovable property etc. Cash etc).

iv. I confirm that as far as I am aware, Mr./Mrs./Ms..____is not engaged in or has never engaged in any such activity which may generate illegitimate funds nor is he/she connected with any activity which is illegal or unlawful, and any wealth that he/she has accumulated is not in breach of money laundering regulations.

Kindly note that the above opinion provided is given in confidence and is furnished as a matter of business courtesy on the express understanding that no responsibility is assumed by me whether in tort, contract or otherwise.

Yours faithfully,

_____

**[Seal]**

## ANNEX IX

## SPECIMEN THIRD PARTY RELIANCE TEMPLATE

Name of Customer: ……..

Address of Customer: ……..

(*including postcode)*

……

I/We certify that in accordance with the provisions of the Financial Intelligence and Anti Money Laundering Act 2002, the Financial Intelligence and Anti-Money Laundering Regulations 2018 and the Anti-Money laundering and Countering the Financing of Terrorism Handbook 2020 as amended from time to time, or equivalent legislation, code or guideline that:

1. I/We have undertaken and completed Customer Due Diligence measures for the Customer and confirm that I/we have:
   (i) Identified and verified the identity of the Customer;
   (ii) Identified and verified the beneficial ownership and control structure of the Customer (where applicable).
   (iii) Understood and obtained adequate and relevant information on the purpose and intended nature of the business relationship or occasional transaction (as applicable).

2. Original or certified copies of Customer Due Diligence documentation shall be made available to [Name of Licensee in Mauritius] upon request without delay.

3. The Customer (s) is/are applying on his/her own behalf and not as nominee, trustee or in a fiduciary capacity for any other person.

4. I/We am/are unaware of any activities of the Customer that cause me/us to suspect either that the applicant is engaged in money laundering or any other form of criminal conduct.

5. I/We are regulated and supervised for the purposes of combating money laundering and terrorist financing and have measures in place for compliance with Customer Due Diligence and record keeping requirements.

Full Name of Regulated Introducer: .....

Name of Regulator: .....Country of Regulator: .....

Registration No: .....

Signed: ..... Full Names: .....

Job Title: ..... Date: .....