NEXUS FINTRADE

AML-CFT COMPLIANCE MANUAL

NEXUS FINTRADE INTERNATIONAL LTD

VERSION: 1.0 - JULY 2026

NEXUS FINTRADE INTERNATIONAL LTD
REGISTERED OFFICE: SUITE 803, 8TH FLOOR, HENNESSY TOWER, POPE HENNESSY STREET,
PORT LOUIS 11328, REPUBLIC OF MAURITIUS
LICENSE NUMBER: GB25205239 | REGISTERED AND REGULATED BY FINANCIAL SERVICES COMMISSION (THE "FSC") IN MAURITIUS

Table of content

INTRODUCTION

NEXUS FINTRADE INTERNATIONAL LTD ("the Company") shall be incorporated under the Laws of Mauritius a Global Business Corporation and is applying for an Investment Dealer (Full Service excluding underwriting) licence from the Financial Services Commission ("FSC").

In 2002, the Financial Intelligence and Anti Money Laundering Act (FIAMLA) was enacted in Mauritius to deal with the prevention of money laundering and the financing of terrorism. The anti-money laundering and combatting financing of terrorism framework of Mauritius was set by FIAMLA and later the Financial Intelligence and Anti Money Laundering Regulations 2003. The regulations of 2003 were amended in 2018 and are now known as the Financial Intelligence and Anti Money Laundering Regulations 2018.

The Company falls within the definition of a reporting person as defined under Section 2 of the FIAMLA 2002. The Company has to ensure ongoing compliance with relevant requirements of the FIAMLA 2002, FIAML Regulations 2018, the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Act 2019 and other rules, regulations, circular letters, codes or guidelines as issued by the FSC from time to time.

The FCC Act received Presidential assent in December 2023 and was proclaimed on 29 March 2024, except for Section 166(9)(g). The FCC Act establishes the Financial Crimes Commission (FCC) as an independent body corporate. The FCC's mandate is to detect, investigate, and prosecute financial crimes, including corruption offenses, money laundering, fraud, and financing of drug dealing. It operates both domestically and internationally for cases linked to Mauritius.

(i)The FCC Act covers the following type of offenses:

(ii)Corruption Offenses: including bribery by public officials, influencing decisions of public bodies, and corruption within private entities;

(iii)Money Laundering Offenses;

(iv)Fraud Offenses: including various forms of fraud, such as false representation, failing to disclose information, and electronic fraud;

(v)Financing of Drug Dealing Offenses; and

(vi)Any offenses connected to financial crimes.

The FCC Act repeals the Prevention against Corruption Act (POCA) 2002, the Assets Recovery Act (ARA) 2011 and part of the Financial Intelligence and Anti-Money Laundering Act (FIAMLA), to ensure that all the functions and powers once conferred to such institutions as the Financial Crimes Commission ('FCC'), the Asset Recovery Investigation Division of the Financial Intelligence Unit or the Integrity Reporting Services Agency have now been absorbed into the FCC. It is also a consolidating act, grouping corruption, money laundering, fraud, financing drug dealing offences and other offences, previously dispersed throughout the repealed enactments mentioned above, under the concept of 'financial crime.'

Legal persons anow have the obligation to put into place adequate procedures to prevent themselves or any other person acting on the legal person's behalf to commit a financial

crime offence under the Act. The FCC Act also provides the new framework for the recovery and confiscation of proceeds, instrumentality of offences or terrorist properties. It provides for both a criminal-based and a civilbased asset recovery regime with the possibility to apply for attachment or confiscation orders. While the criminal-based regime requires a charge, a conviction, or an ongoing criminal enquiry, a civil attachment order can be sought even against a person who is not in Mauritius and was acquitted of an offence, if the proceedings are stayed or if the charge against them was withdrawn before the return of a verdict. The FCC Act describes in detail the different acts that would constitute corruption, money laundering offences, fraud, financing drug dealing offences and specifies the penalties applied in each case.

The Company is committed to ensure its business activities are conducted in compliance with the applicable legal and regulatory standards. The Anti-money laundering and combating financing of terrorism Compliance Manual (thereafter referred to as the AML-CFT Manual or Compliance Manual or Manual) is intended to ensure compliance with the requirements set forth in the FCC ACT, FIAMLA, the Financial Intelligence and Anti Money Laundering Regulations 2018, the UN Sanctions Act 2019 and all other applicable laws and subsidiary legislations. The aim of the AML-CFT Manual is to enable the Company and its employees to apply the measures prescribed by its regulator, the FSC, in terms of Anti-Money Laundering and Combating Financing of Terrorism (AML-CFT), and therefore prevent any violations.

This AML-CFT Compliance Manual reflects the state of the law as at this date. It shall hence be reviewed no less frequently than annually, to ensure its adequacy and effectiveness as well as to reflect any changes in the applicable law and regulations. The Board of Directors will approve all changes made to this Manual. In the event of any inconsistency between this manual and the applicable laws and regulations or rules, codes, guidelines or similar instrument issued by the FSC or any other regulatory authority, the laws, regulations, rules, codes, guidelines shall prevail over this manual.

This AML-CFT Compliance Manual is applicable to the Company and all its subsidiaries, current and future. Employees, including representatives/agents, who are involved in the delivery of prescribed services are expected to know and understand the contents of this Policy and to abide by the standards therein. Any employee found to be acting in breach of this Policy will be subject to disciplinary actions as may be deemed fit by the Board of Directors.

All relevant employees of the Company shall be required to sign the acknowledgment form provided in Annex 9 to demonstrate that the Manual has been circulated to them and that they have read, understood and undertake to adhere by the requirements of the Manual.

1. DEFINITIONS AND INTERPRETATION

AML-CFT	means Anti-money Laundering and Combating the Financing of Terrorism.
Client	means any individual or legal person or legal arrangement that seeks to form a business relationship or to carry out a one-off transaction with/through the Company
Beneficial Owner	means the natural person who ultimately owns or controls a legal person or legal arrangement and/or the individual on whose behalf a transaction is being conducted. It includes the natural person who exercise ultimate control over a legal person or arrangement and such other natural persons as specified below – (A) having ultimate controlling ownership interest in a legal person (B) where there are doubts with regards to (A), the natural person with controlling ownership interest or the natural person exercising control of the legal person through other means (C) where no natural person is identified under (A) or (B), the identity of the natural person who holds the position of senior managing official.
Business relationship	means a contractual relationship between the Company and a client for the provision of products or services by the Company to the client on a frequent, habitual regular, or one-off basis.
CDD	means Customer Due Diligence.
Designated party	means any individual, group, undertaking or entity declared as designated party by the Secretary for Home Affairs following direction by the National Sanctions Committee under section 9 or 10 of the UN Sanctions Act.
EDD	means Enhanced Due Diligence.
FIAMLA	means The Financial Intelligence and Anti-Money Laundering Act 2002.
FIAMLR	means The Financial Intelligence and Anti-Money Laundering Regulations 2018.

FIU	means Financial Intelligence Unit established under section 9 of FIAMLA.
FCCA	Financial Crime Commission Act 2023
FSC Handbook	means the AML/CFT Handbook issued by the FSC
Legal person	means (a) any entity, other than a individual, that can establish a permanent business relationship with the Company or otherwise own property; (b) and includes a company, a foundation, an association, a limited liability partnership, or such other entity as may be prescribed by the FIU or a competent regulator/authority.
Legal arrangement	means a Trust or similar arrangement.
Listed party	means any individual, group, undertaking or entity listed by or under the authority of the United Nations Security Council on the United Nations Security Council Consolidated List- also known as the UN Sanctions List.
MLRO	means Money Laundering Reporting Officer.
ML/TF	means money laundering, terrorist financing and proliferation financing.
Individual	means a living human being with legally capable of entering into a binding contract with the Company (or its subsidiaries).
NRA	means the National Money Laundering and Terrorist Financing Risk Assessment of Mauritius Public Report issued by the Ministry of Financial Services and Good Governance in August 2019.
PEP	means Politically Exposed Person. Politically Exposed Persons are individuals who are or have been entrusted with prominent public functions/positions (for example Heads of State or Heads of government, senior politicians, senior government/judicial/ military officials, senior executives of state owned corporations and important political party officials) as well as their relatives and associates. This includes i. individuals who meet the definition of a PEP in Mauritius (domestic PEP), ii. individuals who meet the definition of a PEP in a foreign country (foreign PEP) and iii. individuals who have been entrusted with a prominent function/position by an international organization, including member of senior

management or other functions equivalent to directors, deputy directors and member of the Board of directors (international organization PEP).

This also includes close associates and family members of PEPs as defined below:

Family members

(a) means an individual who is related to a PEP either directly through consanguinity, or through marriage or similar civil forms of partnership; and

(b) includes any other person as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

Close associates

(a) means an individual who is closely connected to a PEP, either socially or professionally; and

(b) includes any other person as may be specified by a supervisory authority or regulatory body after consultation with the National Committee;

Principals

means any person, whether an individual or a legal person, who either directly or indirectly:

(i) is able to control, or exert significant influence over the business or financial operations of a legal person/ legal arrangement,

(ii) has the power to appoint or remove a member of the governing body of the legal person/ legal arrangement,

(iii) may appoint or remove a person to be a member of the governing body of the legal person/ legal arrangement,

(iv) is a beneficial owner of the legal person/ legal arrangement,

(v) has endowed a legal person/ legal arrangement with its initial assets,

(vi) has transferred property or made a testamentary disposition to a legal person/ legal arrangement.

	For the avoidance of doubt where the client is a company, Principals means: Directors, shareholders, beneficial owner(s) and authorised representatives. Where the client is a partnership, Principals means: the General partner(s), Limited partner(s), beneficial owner(s) and authorised representatives. Where the client is a Trust, Principals means: the settlor, the trustee, the beneficiary(ies), the enforcer and/or protector (if any) and authorised representatives of the trustee. Where the client is a Foundation, Principals means: the founder, members of the Council, the beneficiary (ies), and authorised representatives. Where the client is a "société", Principals means: the "gérant", the "associés", the "bénéficiaire effectif" and authorised representatives
Regulation	means regulation under under Financial Intelligence and Anti-Money Laundering Regulations 2018.
STR	means Suspicious Transaction Report.
The Company	means NEXUS FINTRADE INTERNATIONAL LTD
UN Sanctions Act	means The United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019
UN	means the United Nations organization founded in 1945.
UN Sanctions List	means the United Nations Security Council Consolidated List.

Throughout this Policy use of the masculine, feminine or neuter genders shall be interpreted to include the other genders, and the use of the singular shall be interpreted to include the plural and vice versa.

2. MONEY LAUNDERING, TERRORISM FINANCING, AND PROLIFERATION FINANCING

Money laundering may be described as the process of disguising the origin of proceeds of crime by, for example, passing it through a complex sequence of bank transfers or commercial transactions, with the ultimate aim of making the illicitly earned proceeds appear legal. Money laundering is often wrongly regarded as an activity associated only with organised crime and drug trafficking. However, money laundering occurs whenever a person (natural or legal) deals with direct or indirect proceeds of any act or omission that is in violation of law, be it blackmail, theft, fraud, tax evasion, kidnapping, bribery, copyright infringement, creative accounting etc. Even though the offence is termed as "money laundering" it involves any form of tangible or intangible forms of property, and not only cash, that directly or indirectly represent benefit from crime.

Money laundering is usually described as a three-stage process:

1. **Placement**: the initial stage where the illicit funds are injected into the legitimate financial system. For example by depositing small amounts into bank accounts, or using false invoicing methods. This stage serves two purposes: (i) it relieves the criminal of holding and guarding large amounts of cash; and (ii) it introduces the illegal funds into the legitimate financial system.

2. **Layering:** the primary purpose of the layering stage is to separate the illicit funds from the initial crime by using complex structures and transactions (layers) to obscure the audit trail. For example, the money launderers may begin by moving the funds electronically from one country to another, convert the cash into monetary instruments or enter into loan back arrangements.

3. **Integration:** the final stage of the money laundering scheme. The funds have been fully assimilated in the legitimate economy allowing the criminal to regain the funds in an apparently legitimate transaction. For example by purchasing property, or investing in securities markets.

Terrorism financing

Terrorism financing on the other hand is the process of collecting or providing funding or non-financial support to terrorist organisations. These organisations require financing not only to fund specific terrorist operations, but also to meet the organisational costs of developing and maintaining a terrorist group and to create an enabling environment necessary to sustain their activities. Terrorist organisations may raise funding from legitimate sources, including by the abuse of charitable entities or legitimate businesses or self-financing by the terrorists themselves. Terrorists also derive funding from a variety of criminal activities[1].

The main differences between money laundering and terrorist financing are:

[1] Excerpts from the Executive Summary of the Financial Action Task Force Terrorist Financing Typologies Report published on 29 February 2008.

- in the case of money laundering the funds/assets always origininate from unlawful activities whereas in the case of terrorist financing the funds/ assets can originate from both legal and criminal sources; and

- the underlying objective of the money launderer is to conceal the source of the illicit funds/assets while persons involved in the financing of terrorism aim at concealing that they are funding acts of terror or terrorist organisations.

There are also similarities between money laundering and terrorist financing; these include:

- Criminal activity-terrorists also engage in other forms of crimes, such as drug or human trafficking for example, to fund their activities;

- Both money launderers and terrorist financiers use financial institutions and financial services professionals.

Proliferation Financing

Proliferation refers to the development and use of nuclear, chemical, or biological weapons – also known as weapons of mass destruction, and their delivery systems, in violation of international agreements and export control regimes[2].

Proliferation financing refers to the financing of proliferation of weapons of mass destruction including but not limited to 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. Persons who participate in proliferation and proliferation financing schemes use complex networks of front companies and diversion techniques copied from money launderers to access the global financial system and evade increasingly stringent counter-proliferation financing measures.

3.1. Money Laundering & Terrorism Financing offences:

The main legislations dealing with the offences of Money Laundering, Terrorism Financing and Proliferation Financing in Mauritius are the Financial Crime Commission ACT (FCC Act): Financial Intelligence and Anti-Money Laundering Act 2002 , the Prevention of Terrorism Act 2002, and the The United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 respectively.

3.1.1. Financial Crime Commission ACT (FCC Act):

Section 39:

1) Any person who -
    a) engages in a transaction that involves property which, in whole or in part directly or indirectly, represents the proceeds of any crime; or

[2] National Sanctions Secretariat. (August 2020). *Guidelines on the Implementation of Targeted Financial Sanctions Under The United Nations (Financial Prohibitions, Arms Embargo And Travel Ban) Sanctions Act 2019*

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

crime,

where he suspects or has reasonable grounds to suspect that the property is

derived or realized, in whole or in part, directly or indirectly from any crime, shall

commit an offence and shall, on conviction, be liable to a fine not exceeding 20 million rupees and to penal servitude for a term not exceeding 10 years..

3.1.2.Prevention of Terrorism Act 2002 (POTA)*:*

Section 6:

(1) Any person who, in any manner or form-
(a) solicits support for, or tenders support in relation to, an act of terrorism, or
(b) solicits support for, or tenders support to, a proscribed organisation,
shall commit an offence.

(2) For the purposes of subsection (1), "support" includes-
a) instigation to the cause of terrorism;
b) (i) offer of material assistance, weapons, false documentation or identification;
c) the provision of, or making available; such financial or other related services.

Section 15:

(1) Any person who enters into, or becomes concerned in, an arrangement which facilitates the retention or control by, or on behalf of, another person of terrorist property, in any manner, including-
(a) by concealment;

(b) by removal from the jurisdiction; or

(c) by transfer to any person,

shall commit an offence.

Section 32:

Any person who commits an offence under sections 6 or 15 shall, on conviction, be liable to penal servitude for a term of not less than 3 years nor more than 20 years.

3.1.3.The United Nations(Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 (UN Sanctions Act)

Section 23 (1):

Subject to this Act, no person shall deal with the funds or the assets of a designated party or listed party, including-

(a) All funds or other assets that are owned or controlled by the designated party or listed party, and not just those that can be tied to-
    (i) a particular terrorist act, plot or threat;
    (ii) a particular act, plot or threat of proliferation;

(b) those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly by the designated or listed party;

(c) funds or other assets derived or generated from funds or other assets owned or controlled, directly or indirectly, by the designated party or listed party, and

(d) funds or other asstes of a party acting on behalf of, or at the direction of, the designated party or listed party.

Section 23 (5):

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

3.2. Understanding the risk

Criminal activity generates massive amounts of illicit funds that must be integrated into the legitimate economic and financial system to benefit the criminals without attracting attention to the underlying crime.

Following the National Risk Assessment ("NRA"), Investment Dealers holding the Investment Dealer have been rated as Medium risk in terms of money laundering vulnerability. It was further provided in the NRA that Investment Dealers business activities are characterised by a large number of retail clients and that the complexity of products as well as the customer types (PEPs or clients from high-risk jurisdictions) may pose risks from an AML/CFT perspective.

As mentioned earlier terrorist organisations raise funds both from legitimate and criminal sources to support their activities. Hence, terrorist financing may also entail money laundering.

3. COMPLIANCE OBLIGATION

Since the Company falls within the definition of reporting person under FIAMLA, the Company has a legal obligation to comply with the requirements laid out in both FIAMLA and FIAMLR.

Section 3(2) of FIAMLA states that a reporting person who fails to take such measures as are reasonably necessary to ensure that neither he, nor any service offered by him, is

capable of being used by a person to commit or to facilitate the commission of a money laundering offence or the financing of terrorism shall commit an offence.

The applicable penalty on conviction is a fine not exceeding 10 milion rupees and penal servitude for a term not exceeding 20 years.

Breach by Employee

All employees and officers of the Company shall ensure prompt adherence to the relevant provisions of this Manual. In case any employee or officer breaches requirements laid down in this Manual, the Company may, at its discretion and depending on certain factors (such as the severity and consequences of the breach) take measures including but not limited to initiating disciplinary procedures, and/or reporting the matter to relevant authorities among others.

4. KEY AML-CFT OFFICERS

It is the Company's Policy to ensure its business activities are conducted in compliance with the applicable legal and regulatory standards. In its capacity as reporting person, the Company shall comply with its obligations under the FIAMLA, and FIAMLR.

Therefore, the Company shall appoint a Compliance Officer, a MLRO and Deputy MLRO and establish procedures including but not limited to:

- Identify and verify the identity of clients;
- Ensure proper reporting of suspicious transactions;
- Ensure adequate screening of clients and prospective employees;
- Independent audit function to test the AML/CFT program
- Provide appropriate training to employees on AML-CFT; and
- Maintain documentary evidence of compliance with the legal and regulatory requirements in terms of AML-CFT.

4.1. Compliance officer

Pursuant to Regulation 22 (1) (a), 22 (2) and 22 (3), and relevant provisions of the AML/CFT Handbook, the Company has an obligation to appoint a Compliance Officer who shall have the duties outlined in paragraph 4.1.1 below. The Company shall seek the prior approval of the FSC before appointing a Compliance Officer.

4.1.1 Duties of Compliance Officer

The Compliance Officer shall be responsible for:

(a) Ensuring continued compliance with the requirements of FIAMLA and FIAMLR subject to the continuous supervision of the Board and senior management,
(b) Undertake day-to-day management of the AML-CFT programme of the Company,
(c) Regularly report to the Head of Company on the status of compliance and/or non-compliance,
(d) Contribute to designing, implementing and maintaining the internal AML-CFT compliance manuals, policies and system of the Company.

In other words and from a practical perspective, the Compliance Officer shall be the focal person responsible for AML/CFT Compliance of the Company.

The Company shall ensure, at all times, that the Compliance Officer:

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

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

(c) has the full co-operation of the financial institution staff;

(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 FIAMLA and FIAML Regulations 2018, and this Handbook are being met and that the financial institution is taking sufficiently robust measures to protect itself against the potential risk of being used for ML and TF.

Additionally, the Company shall seek the prior approval of the FSC in accordance with Section 24 of the Financial Services Act 2007 before appointing him. The Company shall also ensure that, even after appointing the Compliance Officer, the latter remains fit and proper for the position.

4.2. MLRO

Pursuant to Regulation 26 (1), the Company must appoint a MLRO to whom all internal suspicious transactions report shall be made, and a Deputy MLRO who shall perform the duties of the MLRO in his absence.

In line with Regulation 26(4) of FIAMLA Regulations and relevant provisions of the Guidelines, the MLRO and the Deputy MLRO of the Company must:

(i) be of sufficiently senior status in the Company or have sufficient experience and authority, and

(ii) have a right of direct access to the Board of directors of the Company and have sufficient time and resources to effectively discharge his functions.

The same individual may be appointed to the positions of MLRO and Compliance Officer, provided (i) it considers this appropriate with regard to the respective demands of the two roles and (ii) the individual to be appointed has sufficient time and resources to fulfil both roles effectively.

Both the MLRO and DMLRO should be registered as active users on the GoAML platform of the Financial Intelligence Unit (FIU) as soon as they have been approved in this capacity and throughout their appointment.

4.2.1 Duties of the MLRO

The MLRO must be given access to all the relevant information or records to investigate whether a reported transaction is suspicious or not. For the purpose of the investigation, the MLRO shall consider all relevant information available to him to determine whether or not the reported transaction is suspicious or not. The MLRO shall be the focal point of contact for the FIU as well.

The MLRO and DMLRO shall be registered on the GoAML platform of the FIU and the evidence of such registration shall be kept on records and made available to the regulatory authority upon request.

Handling Suspicious Transaction Reports

As soon as the MLRO or the DMLRO receives an Internal STR, he shall make an entry in the STR log (*refer to Annex 3*) along with all the details. Pursuant to Regulation 27 (e) the MLRO must be given access to all the relevant information or records to assess whether the transaction is suspicious or not.

Section 14(1) of the FIAMLA provides that the reporting person shall make a Suspicious Transaction Report (STR) to the FIU as soon as practicable **but not later than 5 working days** from the day on which he became aware of the suspicious transaction. The MLRO shall document the information that was examined to assess the transaction reported. In compliance with Regulation 30 (3) the date the STR was made to the FIU must be documented in the STR Log. In case where the Company is in the process of filing a STR, it may seek advice from the FIU about how to handle the customer, or whether they can halt the transactions without tippping off the latter.

If after examination, the MLRO considers that the transaction reported is not suspicious, he shall document the information that was examined to assess the transaction as well as the reasons for not making a report to the FIU in the STR Log. Documenting the information may include having a file (physical or electronic) to which only the MLRO or Deputy MLRO shall have access and recording the following documents/information into it:

- Facts which relate to the alleged suspicious activity / transaction
- Documents / evidences / information relating to the internal investigation conducted by the MLRO or Deputy MLRO
- Findings of the internal investigations
- Written minutes of meetings held with employees during the internal investigations (if any)
- Written analysis from the MLRO / Deputy MLRO substentiating the decision to file or not to file a STR to the FIU

Note that the above is a non-exhaustive list.

The MLRO of the Company should be the main point of contact of the Company with the FIU. The officers and employees of the Company are strictly prohibited from disclosing to any person information or any other matter which is likely to prejudice an investigation on a suspicious transaction.

All employees shall be made aware of the identity of the Compliance Officer, the MLRO and the DMLRO. In the event there is a change in MLRO or DMLRO, the officers and employees of the Company must be notified accordingly. The Deputy MLRO shall assume the duties and responsibilities of the MLRO regarding suspicious transaction reporting and shall be granted the same access to information and documentation to enable him to perform his duties in the absence of the MLRO.

5. AML-CFT RISK ASSESSMENT

Section 17 of the Financial Intelligence and Anti-Money Laundering Act 2002 ("FIAMLA") requires every reporting person to take appropriate steps to identify, assess and understand the money laundering and terrorism financing risks for customers, countries or geographic areas and products, services, transactions or delivery channels. Section 17 compels reporting persons to consider all relevant risk factors before determining the level of overall risk, the suitable level and type of mitigation to be applied. The nature and extent of the assessment must match the nature and size of the business of the reporting person and must take into consideration: -

(a) all relevant risk factors including –

(i) the nature, scale and complexity of the reporting person's activities;

(ii) the products and services provided by the reporting person;

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

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

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

(vi) technological developments; and

(b) the outcome of any risk assessment carried out at a national level and any guidance issued.

Reporting persons are also expected under section 17 to identify and assess the money laundering or terrorism financing risks that may arise in relation to the launch of a new product or business practice or the use of a new or developing technology

Based on section 17 FIAMLA a business risk assessment is the process by which a reporting person ascertains and evaluates how vulnerable it is to getting involved in ML/TF in order to implement appropriate controls and measures to minimise and manage those risks. A business risk assessment is intended to assist the reporting person to identify the extent to which its business, products and services are exposed to ML /TF. A proper business risk assessment should enable the Company to make sure that its AML-CFT framework is equivalent and targeted to the ML/TF risks it faces.

5.1. Business Risk Assessment

The objective of a business risk assessment is to identify the extent to which the Company's business, products and services are exposed to ML /TF. Under section 17 (2) of FIAMLA six key areas must be taken into consideration when undertaking a business risk assessment amongst other risk factors:

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

In addition, reporting persons are also required to take into account the outcome of any risk assessment carried out at a national level and any guidance issued. Hence, the findings of the National Risk Assessment report must be taken into consideration.

5.1.1. Business risk Assessment guidelines

Therefore, the Company, in its capacity as reporting person and therefore a reporting person, shall take appropriate measures to conduct a business risk assessment as required under section 17 of FIAMLA.

The business risk assessment methodology has been included in the same document as the business risk assessment itself. Kindly refer to this document accordingly (refer to Annex 7).

As part of the Business Risk Assessment, the below risk factors shall be taken into consideration:

<u>The nature, scale and complexity of activities</u>

• Consider the services provided by the business and how those services might be abused for ML/TF.

• Actively involve all members of senior 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. However, this will also depend on the assessment of the area of operations and nature of business. As a whole, factors need to be considered together in order to have a more comprehensive assessment.

• Consider the jurisdictions in which the business operates, any particular threats from those jurisdictions, any particular vulnerabilities within the organisation in those jurisdictions. Regulation 24(1) of the FIAML Regulations 2018 states how high risk third countries should be identified.

Products and Services Provided by Financial Institutions

• 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.

Section 17A(b) FIAMLA prescribes that every reporting person must regularly review, update and, where necessary, enhance the, policies, controls and procedures established. Therefore, the Business Risk Assessment conducted shall be reviewed at least annually to consider the extent of exposure of the Company to ML/TF risks.

The nature, scale, complexity and location of customers 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.

5.2. Customer Risk Assessment

The risks associated with a customer is determined by the significance of risk indicators. In compliance with section 17(1) FIAMLA, based on the identification documents collected and result of screening, an AML-CFT customer risk assessment shall be done. For this purpose a customer risk assessment shall be conducted using the Customer Risk Assessment Tool to determine the level of ML/TF risks associated with doing business with the client. Kindly refer to the Customer Risk Assessment tool accordingly (refer to Annex 8).

5.2.1. Customer Risk Assessment Process

Based on the information collected from the identity verification process and details captured during interaction with the customer, the user of the Customer Risk Assessment Tool will need to assess the risks by completing same.

The risk assessment levels will be categorized according to the below:

Risk Level	Frequency of Review
Low	3 years
High	Annually

Risk Factors

Different risk factors have been taken into consideration in the customer risk assessment matrix. A guidance (also forming part of the risk assessment methodology used) has been provided below for better understanding:

Basic risk factor categories are:

1. Customer risks (individual/entity)
2. Geographical risks
3. Products/services risks
4. Any adverse information captured during screening

Customer Risks

Customer risk is associated to any factors related to customers activity, reputation, nature or behaviour that might increase ML/TF risks.

When identifying the risk associated with customers the Company considers the customer's and the customer's beneficial owner's business or professional activity, reputation, structure, nature and behaviour.

Risk factors to be considered based on customer **activity**:

- Does the customer or beneficial owner have links to sectors that are commonly associated with higher corruption risk, such as construction, pharmaceuticals, healthcare, the arms trade and defence, the extractive industries or public procurement?
- Does the customer or beneficial owner have links to businesses to any product or activity deemed illegal under host country laws or regulations or international conventions and agreements, including without limitation host country requirements related to environmental, health and safety and labour aspects?
- Does the customer or beneficial owner have direct links to businesses that fall outside of the Company's risk appetite. For example, is related to crypto currency businesses via ownership structure or partnership, non-licensed businesses that does require license etc.
- Does the customer or beneficial owner have links to sectors that are associated with higher ML/TF risk, for example certain financial institutions, gambling, betting, casinos or Forex trading?

- Does the customer or beneficial owner have links to businesses that involve significant amounts of cash (cash make up more than 30% of all transactions)?
- Where the customer is a legal person or a legal arrangement, what is the purpose of their establishment? For example, what is the nature of their business?
- Does the customer have political connections, for example, are they a Politically Exposed Person ("PEP") or is their beneficial owner a PEP? Does the customer or beneficial owner have any other relevant links to a PEP, for example, relatives or close associates PEPs? Are any of the customer's directors PEPs and, if so, do these PEPs exercise significant control over the customer or beneficial owner?
- Is natural or a legal person subject to enforceable disclosure requirements that ensure that 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?
- Is the customer a financial institution acting on its own account from a jurisdiction with an effective AML/CFT regime and is it supervised for compliance with local AML/CFT obligations?
- Is there evidence that the customer has been subject to supervisory sanctions or enforcement for failure to comply with AML/CFT obligations or wider conduct requirements in recent years?
- Is the customer a public administration or enterprise from a jurisdiction with low, medium or high levels of corruption?
- Is the customer's or the beneficial owner's background consistent with what the Company 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?
- If the customer is a legal entity whose business profile is related to money business have sufficient AML/CTF policies and procedures in place to monitor their own customers.

Risk factors to be considered based on customer **reputation**:

- Are there any adverse media reports or other relevant sources of information about the customer, for example are there any allegations of criminality, bribery or terrorism and other financial crimes against the customer or the beneficial owner? If so, are these sources reliable and credible? The Company 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. The absence of criminal convictions alone may not be sufficient to dismiss allegations of wrongdoing.
- 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 terrorist financing? Does the Company 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?
- Has the customer or beneficial owner been the subject of a suspicious transactions report in the past?
- Was there 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?
- Are there any other customer behavioural issues that arise like unwillingness to provide or provide false company information or documentation?

Risk factors to be considered based on customer **nature and behaviour**:

- Does the customer have legitimate reasons for being unable to provide robust evidence of their identity, perhaps because they are an asylum seeker?

- Are there any doubts arising about the veracity or accuracy of the customer's or beneficial owner's identity?
- Are there any 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?
- 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?
- Does the customer issue bearer shares?
- Does the customer have nominee shareholders?
- Is the customer a legal person or an arrangement that could be used as an asset-holding vehicle?
- Is there a sound reason for changes in the customer's ownership and control structure?
- Does the information and documentation provided by the customer correlate with information provided in independent public source?
- Does the customer request unnecessary or unreasonable levels of secrecy? For example, is the customer reluctant to share CDD information (customer's name, photograph on an official document and residential address), or do they appear to want to disguise the true nature of their business?
- Can the customer's or beneficial owner's or legal person source of wealth or source of funds be easily explained, for example through their occupation, inheritance, financial documents, investments? Is the explanation plausible?
- Does the customer use the products and services they have taken out as expected when the business relationship was first established?
- Where the customer is a non-resident, could their needs be better serviced elsewhere? Is there a sound economic and lawful rationale for the customer requesting the type of financial service sought?
- If it is known publicly that customer company received warnings of fines? If so, were the fines / warnings related to financial crimes/financing terrorism? Were there any possible relations to criminal activities or it was just was unintentional legal violation? How the company was acting? What were further actions/reactions of that company after the warnings/fines were received? Example: accepted and followed the provided recommendations to complete the legal requirements?
- Whether the customer official website is active and looks legitimate according to the nature of business that customer conducts.

Possible factors that that the Company uses/implements to mitigate risk the risk for e-money products:

- In order to avoid any financial or reputational damage to the Company possibly caused by its customers, every new customer (natural or legal person) go through several levels of protective measures. Starting with electronic identification and documents submission, all customer information is carefully checked though CDD procedure and customer information screening against PEP/Sanctions lists, adverse media search, customer risk evaluation, performed by AML specialist and second level of review performed by MLRO before granting an access to a customer into THE COMPANY systems. After customer is onboarded according to the risk category assigned his KYC data and activity is being assessed periodically (Low – every 3 years, medium – every 2 years, high – every 1 years or less) by AML specialists and depending on the results received – certain actions taken (e.g. KYC updates, customer explanations requested, customer off-boarding); As well customer information is screened daily against sanctions and PEP lists;
- As a part of CDD procedure during customer onboarding process – it is obligatory for every finance business related potential client to prove the presence of effective AML processes and procedures performed on their clients and provide evidence;

- Correct rules applied to customer transaction monitoring system that trigger any customer activity change or unexpected behaviour (sudden usage of products like prepaid cards overseas, transactions from different IP addresses, significant amounts of transactions just below the threshold, large amount transactions, transactions coming from or being sent to many different accounts etc.) and create alerts;

Often changes in customer personal details (identification, IP, linked bank accounts) like any other changes in client information are recorded and audit trail with information about mentioned changes are be visible for AML specialists conducting customer periodical reviews. If changes are significantly frequent customer can be contacted and requested for KYC profile update.

Geographical risks

Country risk refers to any geographical locations, jurisdictions or relations with jurisdictions that may pose ML/TF risk.

- When identifying the risks associated with countries and geographical areas, the the Company considers jurisdictions in which the customer and beneficial owner are based, places where business is being conducted, affiliations, other relevant personal links, public source information about the jurisdictions where affairs related to any kind of financial crime, terrorism, briberry and corruption recently took place. The Company has own internal country risk ratings set following multiple reliable and credible sources (Wolfsberg, FATF, Country Corruption Index, TF index, KYC etc.). And according to these ratings that include all mentioned risks based on the jurisdiction (ML, TF, Bribery/corruption/tax-avoidance) set due diligence procedures for customers.

In order to evaluate the risks general rules to be considered:

- Where the funds used in the business relationship have been generated abroad, the level of predicate offences to money laundering and the effectiveness of a country's legal system will be particularly relevant;
- Where funds are received from, or sent to, jurisdictions where groups committing terrorist offences are known to be operating, the Company considers to what extent this could be expected to or might give rise to suspicion, based on what the Company knows about the purpose and nature of the business relationship;
- Where the customer is a credit or financial institution, the Company pays particular attention to the adequacy of the country's AML/CFT regime and the effectiveness of AML/CFT supervision;
- Where the customer is a corporate/legal person or trust, the Company takes into account the extent to which the country in which the customer and, where applicable, the beneficial owner are registered effectively complies with international tax transparency standards.

Risk factors to be considered based on **jurisdiction.**

When identifying the effectiveness of a jurisdiction's AML/CFT requirement obligations:

- Has the country been identified as having strategic deficiencies in its AML/CFT requirement obligations (high-risk third country)?
- Is there information from more than one credible and reliable source about the quality of the jurisdiction's AML/CFT controls, including information about the

quality and effectiveness of regulatory enforcement and oversight? Examples of possible sources include mutual evaluation reports by the Financial Action Task Force (FATF) or FATF-style Regional Bodies (FSRBs) (a good starting point is the executive summary and key findings and the assessment of compliance with Recommendations 10 (customer due diligence and record keeping), 26 (regulation and supervision of financial institutions), 27(powers of supervisors) and Immediate outcomes 3 (supervision)and 4 (preventive measures)the FATF's list of high-risk and noncooperative jurisdictions International Monetary Fund (IMF) assessments and Financial Sector Assessment Programme (FSAP) reports. Membership of the FATF or an FSRB (e.g. MoneyVal) does not, of itself, mean that the jurisdiction's AML/CFT regime is adequate and effective.

when identifying the level of terrorist financing risk associated with a jurisdiction:

- Is there information, for example from law enforcement or credible and reliable open media sources, suggesting that a jurisdiction provides funding or support for terrorist activities or that groups committing terrorist offences are known to be operating in the country or territory?
- Is the jurisdiction subject to financial sanctions, embargoes or measures that are related to terrorism, financing of terrorism or proliferation issued by, for example, the United Nations or the European Union?

when identifying a jurisdiction's level of transparency and tax compliance:

- 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 Organisation for Economic Co-operation and Development (OECD), which rate jurisdictions for tax transparency and information sharing purposes; assessments of the jurisdiction's commitment to automatic exchange of information based on the Common Reporting Standard; assessments of compliance with FATF Recommendations 9(Financial institution secrecy laws), 24 (Transparency and beneficial ownership of legal persons) and 25 (Transparency and beneficial ownership of legal arrangements)and Immediate Outcomes 2 (International cooperation)and 5 (Legal persons and arrangements) by the FATF or FSRBs; and IMF assessments (e.g. IMF staff assessments of offshore financial centres).
- Has the jurisdiction committed to, and effectively implemented, the Common Reporting Standard on Automatic Exchange of Information, which the G20 adopted in 2014?
- Has the jurisdiction put in place reliable and accessible beneficial ownership registers?

when identifying the risk associated with the level of predicate offences to money laundering:

- Is there information from credible and reliable public sources about the level of predicate offences to money laundering, for example corruption, organised crime, tax crime and serious fraud? Examples include corruption perceptions indices; OECD country reports on the implementation of the OECD's anti-bribery convention; and the United Nations Office on Drugs and Crime World Drug Report.
- Is there information from more than one credible and reliable source about the capacity of the jurisdiction's investigative and judicial system effectively to investigate and prosecute these offences?
- Is the customer, a company or business partners are located in or the product receives funds from sources in, a jurisdiction associated with lower tax regulations, higher bribery / corruption and ML risks;
- Is the customer, a company or business partners are located in, or the product receives funds from sources in, a jurisdiction associated with higher TF risk;
- Is the customer or a beneficial owner has citizenship of a jurisdiction associated with higher ML/TF risk.

Possible factors which are implemented in the Company to mitigate the risk for e-money products:

- The Company pays particular attention to jurisdictions known to provide funding or support for terrorist activities or where groups committing terrorist offences are known to be operating, and jurisdictions subject to financial sanctions, embargoes or measures that are related to terrorism, financing of terrorism or proliferation.

The customer has to provide a document proving his/her citizenship and place of residence, places of incorporation and operations during an onboarding procedure in order to mitigate the risk arising from possible affiliation with potentially harmful country.

Products/services risks

Products, services and transactions risk relates to any products, services and transactions that might create conditions for ML / TF risks to occur.

When identifying the risk associated with product, service and transactions the Company mainly considers the factors, listed below:

- the level of transparency, or opaqueness, the product, service or transaction affords;
- the complexity of the product, service or transaction;
- the value or size of the product, service or transaction.

For e-money products:

- thresholds;
- the funding method;
- utility and negotiability.

Risk factors to be considered based on **transparency:**

- To what extent do products or services allow the customer or beneficial owner or beneficiary structures to remain anonymous, or facilitate hiding their identity? Examples of such products and services include bearer shares, fiduciary deposits, offshore vehicles and certain trusts, 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;
- To what extent is it possible for a third party that is not part of the business relationship to give instructions?

Transactions

Thresholds: *the product allows:*

- high-value or unlimited-value payments, loading or redemption, including cash withdrawal;
- high-value payments, loading or redemption, including cash withdrawal;
- high or unlimited amount of funds to be stored on the e-money product/account.

Funding method: *the product can be:*

- funded with payments from unidentified third parties;
- funded in various currencies (multicurrency accounts);
- Any anonymous loading of funds is prohibited absolutely.

Utility and negotiability: *the product:*

- allows person-to-person transfers;
- is accepted as a means of payment by a large number of merchants or points of sale;

- is designed specifically to be accepted as a means of payment by merchants dealing in goods and services associated with a high risk of financial crime, for example online gambling;
- can be used in cross-border transactions or in different jurisdictions;
- can be used in various currencies (multicurrency accounts);
- is designed to be used by persons other than the customer, for example certain partner card products (but not low-value gift cards);
- allows high-value cash withdrawals.

Possible factors which are implemented in the Company to mitigate the risk for money products:

Thresholds: the product

- sets low-value limits on payments, loading or redemption, including cash withdrawal (although a low threshold alone may not be enough to reduce TF risk);
- limits number of payments, loading or redemption, including cash withdrawal in a given period;
- limits the amount of funds that can be stored on the e-money product/account at any one time.

Funding: the product

- requires that the funds for purchase or reloading are verifiably drawn from an account held in the customer's sole or joint name at financial institution;

6. CUSTOMER DUE DILIGENCE

On a general note, the Company shall apply normal customer due diligence for prospective customers/customers or enhanced due diligence measures in case of high risk customer relationship. Should there be a low risk in terms of money laundering, the Company may apply simplified due diligence as mentioned below.

Simplified Due Diligence

Applying simplified due diligence does not mean no applying CDD measures but rather applying reduced measures which shall be commensurate with the risk posed by the customer or specific situation.

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

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

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

Simplified CDD shall never apply where, a financial institution knows, suspects, or has reasonable grounds for knowing or suspecting that a customer or an applicant for business is engaged in ML or TF or that the transaction being conducted by the customer or applicant for business is being carried out on behalf of another person engaged in money laundering or where there are other indicators of ML/TF risk. Where simplified CDD measures are adopted, financial institutions should apply a risk-based approach to determine whether to adopt the simplified CDD measures in a given situation and/or continue with the simplified

measures, although these clients' accounts are still subject to transaction monitoring obligations.

6.1. Identity Verification

The Company has a legal obligation to identify its client whether permanent or occasional and verify the identity of its client using reliable, independent source documents, data or information specified by its regulator. In other words identity verification is about ensuring that clients are who they claim to be.

The standard documents to be requested from clients to verify identity are listed in Tables 1 to 3 below. Gathering the required information through the specified documents will allow the Company to:

1. make a profile of the client,
2. assess any ML/TF risk associated with the client,
3. decide whether it wishes to enter into a business relationship with the client or not based on the profile and risk assessment of the client.

6.1.1. Individuals

When the business relationship will be entered into between the Company and an individual acting in his own name, the documents listed in table 1 below shall be requested from the client to comply with Regulation 4:

Table 1- Documents to be requested from clients-Individuals

INFORMATION REQUIRED	SOURCE DOCUMENT	DETAILS
▪ **Full Name (including former names)** ▪ **Date and place of birth,** ▪ **Nationality,** ▪ **Gender** ▪ **Government issued personal identification number or other government issued unique identifier**	▪ National Identity card, or ▪ Current valid passport, ▪ A formal document evidencing change of name (where applicable for example a mariage certificate, a certificate of change of name),	The passport or identity card should bear a photograph and the signature of the individual. If the client has more than one nationality, passports or national identity document under the additional nationality should be requested.
▪ **Current and Permanent Address**	▪ A utility bill (a land line telephone bill/gas bill/electricity bill/water bill) issued within the last 3 months, or ▪ A bank statement issued within the last 3 months, or	P.O Box addresses are not acceptable as permanent residential addresses and may not be accepted. Utility Bills should be in the name of the client. If the document is in the name of a parent (mother or

	▪ A credit card statement issued within the last 3 months, or ▪ A letter from a professional person, such as a lawyer, a certified accountant, a banker or a notary, who knows the individual. The letter should include the permanent residential address of the individual.	father), the Birth Certificate of the client should be provided. If the Utility Bill is in the name of a third party, a letter from the third party should be provided, certifying that the client resides at the address stipulated on the Utility Bill, and a certified copy of the third party's identity card should be provided.
▪ **Occupation and name of employer**	▪ Job title and name of employer, or ▪ CV, or ▪ Nature and details of self-employment where applicable. ▪ For self-employed trade licence and business registration card.	Period (i.e, dates) of employment and name of employer should be indicated in the CV.
▪ **Source of funds to be used by client to finance acquisition or rental**	▪ Relevant supporting evidence (as applicable).	All fields of the form should be completed. The form should be signed and dated by the client.

6.1.2. Legal persons or legal arrangements

In case the business relationship will be entered into between the Company and a legal person or legal arrangement, when the proposal is accepted by the client, the Company is required to verify the following:

i. The name, legal form and proof of existence of the client;
ii. Powers that regulate and bind the client (i.e., who manages the client and who has the right to represent and sign on its behalf);
iii. The names of persons occupying senior management positions in the client; and
iv. The address of the registered office or principal place of business of the client.

The Company should also understand and document the nature of business and ownership control structure of a client which is a legal person or legal structure.

Therefore the identity verification documents listed in Table 2 below must be requested from the client.

Table 2 below lists the standard identity verification documents to be obtained from clients in general. When on-boarding a new client, the client shall be requested to complete and

sign terms and conditions and submit KYC information and documents as requested on the website.

Table 2- Documents to be requested from clients- Legal persons or legal arrangements

Type of legal person/ legal arrangement	Document to be requested
Company	▪ Certificate of incorporation or registration, ▪ Memorandum and Articles of Association or Constitution (as applicable), ▪ Company registry search ▪ Certificate of good standing from a relevant national body, ▪ Business registration card (where applicable), ▪ Shareholding structure chart up to beneficial owner, ▪ Latest Register of directors, ▪ Latest Register of members/shareholders, ▪ Registered office address and principal place of business (where different from the registered office), ▪ Latest audited financial statements or annual report if available, ▪ Identity verification documents on the directors, significant shareholders and on the beneficial owner, ▪ Proof of identity and residential address of individuals authorised to represent the Company for the purpose of the transaction and sign the required documents
Partnership	▪ Partnership agreement or partnership deed, ▪ Certificate of registration of the partnership if it is registered, ▪ Evidence that the partnership continues to exist (Certificate of good standing from registrar) ▪ Latest audited financial statements or annual report, ▪ Identity verification documents on the Managing/General Partner, ▪ Latest Register (or equivalent document) showing the names, addresses and percentage interest of the Limited Partners, ▪ Registered office address and principal place of business (where different from the registered office), ▪ Identity verification documents on the limited partners and the beneficial owner, ▪ Proof of Identity and residential address of individuals authorised to represent the partnership for the purpose of the transaction and sign the documents, and
Société	▪ Acte de société or equivalent document establishing the société, ▪ If the société is registered, certificate of registration,

	▪ Evidence that the société continues to exist, ▪ Ownership/holding structure up to the beneficial owner, ▪ Proof of identtiy and residential address of individual authorised to sign the required documents, ▪ Identity verification documents on the administrators or "gérants" of the "société", ▪ Latest Register (or equivalent document) showing the names, addresses and ownership interest of members or "associés, ▪ Identity verification documents on the members or "associés" in the "société", ▪ Identity verification documents on the beneficial owner, ▪ Latest financial statements or annual report if available, and
Trust	▪ Trust deed or pertinent extracts indicating the names of settlor, trustee, beneficiaries, protector, enforcer, and the proper law of the Trust, ▪ Information from the trustee that the Trust continues to exist, ▪ Information on the type and purpose of the Trust, ▪ Information on the origins of the Trust's assets, ▪ Identity verification documents on the Settlor, trustee, beneficiaries, protector (if any) and enforcer (if any), ▪ Proof of identtiy and residential address of individual authorised to sign the required documents for the acquistion ▪ Details of the registered office and place of business of the trustee ▪ Latest Trust's financial summary or financial statements if available, and
Foundation	▪ Charter and/or Articles of the Foundation, ▪ If the Foundation is registered, certificate of registration, ▪ confirmation from the Foundation's council that the Foundation continues to exist, ▪ Register or equivalent document showing the names and addresses of the members of the Foundation's council, the Founder and any person who has endowed assets to the Foundation, ▪ Details of the Registered office and place of business of the Foundation, ▪ Identity verification documents on Founder, members of Council and beneficiaries of the Foundation, ▪ Latest financial summary or financial statements if available, and

Beneficial Ownership

The Company shall identify and verify the identity of beneficial owners of legal persons or arrangements. In accordance with Regulation 6 of the FIAML Regulations 2018, the identification of beneficial owners shall be done by requesting information on:

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

The identity of the individual who ultimately owns or controls the client (i.e., the beneficial owner) must in all cases be established and verified.

6.1.3. Authorized persons or authorized signatories

Some clients (especially those that are legal persons) will be represented by individuals authorised to act on their behalf. The Company has a legal obligation to verify the identity and current permanent and residential address of any individual who claims to act on behalf of a client. The Company must also verify that such a person is duly authorised to represent or act on behalf of the client. Therefore, the information listed in Table 3 below will need to be obtained from any individual who claims to be acting on behalf of a client.

Table 3- Documents to be requested from authorised persons

INFORMATION	SOURCE DOCUMENT	RECOMMENDATION
▪ **Full Name (including former names)** ▪ **Date and place of birth,** ▪ **Nationality,** ▪ **Gender** ▪ **Government issued personal identification number or other government issued unique identifier**	▪ National Identity card, or ▪ Current valid passport, ▪ A formal document evidencing change of name (where applicable for example a mariage certificate, a certificate of change of name), ▪ The relevant government document such as, but not limited to, any trade licence issued or the Tax Account Number (TAN) of the individual.	The passport or identity card should bear a photograph and the signature of the individual. If the client has more than one nationality, passports or national identity document under the additional nationality should be requested.

▪ **Current and Permanent Address**	▪ A utility bill (a land line telephone bill/gas bill/electricity bill/water bill) issued within the last 3 months, or ▪ A bank statement issued within the last 3 months, or ▪ A credit card statement issued within the last 3 months, or ▪ A letter from a professional person, such as a lawyer, a certified accountant, a banker or a notary, who knows the individual. The letter should include the permanent residential address of the individual.	P.O Box addresses are not acceptable as permanent residential addresses and may not be accepted. Utility Bills should be in the name of the client. If the document is in the name of a parent (mother or father), the Birth Certificate of the client should be provided. If the Utility Bill is in the name of a third party, a letter from the third party should be provided, certifying that the client resides at the address stipulated on the Utility Bill, and a certified copy of the third party's identity card should be provided.
▪ **Written evidence that the individual is authorised to act on behalf of the client**	▪ Signed written resolution authorising the individual to represent the client	The document must specify the name of the individual, how he is related to the client, and mention the property to be acquired, the price and that the individual is authorised to represent the client for the transaction and sign any document necessary for the transaction.

6.2. Original or certified true copies of identity verification documents

As mentioned earlier the Company must identify and verify the identity of its clients using reliable, independent source documents, data or information. Therefore, the Company needs to ensure that the documents it is relying on for identity verification are accurate and that they actually relate to the client.

In case where an employee or officer of the Company had any face-to-face contact with client and verified the original documents, the latter may certify due diligence documents. Apart from this, the verification documents of the client must be certified by a suitable person such as a lawyer, a qualified accountant or other professional person. Professional person may include:

- notary,
- an actuary,
- a qualified accountant,
- a member of the judiciary (a police officer, a judge, a magistrate),
- an employee of an embassy or consulate of the country of citizenship of the person,
- a manager, officer, director or secretary of a financial institution regulated for AML-CFT purposes.

The certifier should indicate that the copy is a true copy of the original document. The certifier must sign the copy and put his stamp (if he has one) on the copy, and clearly indicate his name, address and job title/profession together with his contact details (i.e., a telephone number or address).

6.3. Screening

As part of the identity verification process screening must be conducted on clients and their Principals (when clients are legal persons or legal arrangements). Screening is done by running searches on independent and reliable databases based on the information gathered from the identity verification documents obtained. The Company will be using Refinitiv World check for conducting its screening, including ongoing screening.

The objective of screening is to ascertain whether clients (or their Principals in the case of clients that are legal persons or legal arrangements):

- are Politically Exposed Persons; or
- have any connections to organized crime, drug trafficking, sanction, arms & weapons dealing, human trafficking, foreign official corruption, violent crime, or terrorism; or
- are or have been subject to any convictions or allegations of any fraudulent or criminal/questionable activities.

In the event where complete identity documents have not yet been obtained (example if it is still a prospective customer not yet onboarded), in order not to disrupt the normal conduct of business, screening may be conducted based on the information listed below. However, once the identity verification documents are obtained, the screening results should be verified against the documents to ensure there are no inconsistencies:

For individuals:

- Name (including any former names, any other names used and other aliases)
- Nationality (including any additional nationality)
- Country of residence

For legal persons or arrangements:

- Name (including any former names, any other business or trade names used)
- Country of registration
- Country where business/activity is conducted

Results of the screening conducted should be kept as part of the identity verification records of the client (whether in hard or soft copy) for the duration of the business relationship and for a period of at least seven years after it ends.

If the screening indicate that the client (or any of its Principals):

- Is a Politically Exposed Person; or
- has any connections to organized crime, drug trafficking, sanction, arms & weapons dealing, human trafficking, foreign official corruption, violent crime, or terrorism; or

- is or has been subject to any convictions or allegations of any fraudulent or criminal/questionable activities,

the Company must treat the business relationship as high risk, and apply EDD measures as explained later in this manual. If there is any suspicion that the client might be attempting to use the products/services of the Company to commit ML/TF, an Internal STR (*refer to Annex 3 for template*) must be made to the MLRO who will then assess whether an STR needs to be filed to the FIU.

All screening reports will be kept on their respective customer files/folder.

6.4 Screening Engine

Refinitiv World-Check

Compliance & Risk Management Department will be using the World-Check tool, provided by the company Refinitiv, as the main assisting one. World-Check holds information that helps financial institutions, corporates, professional services firms, governments, law enforcement agencies, regulators and other World-Check customers and companies within the Refinitiv Group to perform due diligence and other screening activities in accordance with their legal or regulatory obligations and risk management procedures carried out in the public interest, including but not limited to the purposes of anti-money-laundering or 'know your customer', anti-bribery or anti-corruption or other regulatory compliance checks, or for preventing, investigating, detecting or prosecuting financial crime, fraud and serious misconduct or dishonesty, or other criminal or unlawful activity (for example, modern slavery, illegal trafficking, environmental crime, etc.) and any unethical conduct.

In this way, compliance officers may perform checks quickly for each customer, vendor, business partner or any other counterparty in relation to three main areas of sources:

a) Official keyworded sources – sanctions lists, regulatory enforcement, law enforcement
b) Media Sources & Adverse Media – news reports, journal articles, archived news aggregators, reputable media sources
c) Government and official sources – court records, election results, company filings, official company websites and press releases.

As always, the company does not want to rely purely on automatic tools due to the experiences with potential gaps or machine misunderstanding that a person (compliance officer) might understand easily. Therefore, each match is manually checked by a qualified (and trained) compliance officer, thus achieving full certainty about the outcome.

In addition to the use of Refinitiv World-Check, the Compliance Officer shall conduct key words searches on internet to ensure that risks of missing any relevant or adverse information is mitigated. All internet searches results shall be kept on records.

6.5 Verification of source of funds

The fact that the funds for the transaction will be remitted from a bank account or a credit/debit card does not exempt the Company from its obligation under section 3(2) of FIAMLA 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.

Source of funds is defined as the activities that generated the funds to be used for the purchase of the plot of land, for example:

- Income from employment
- Income from business activity
- Loan
- Property sale
- Sale of investments
- Gift
- Inheritance
- Sale of business
- Compensation payment
- Return on investments/savings
- Lottery/gambling win

Source of funds may be established through a combination of sources such as information provided by the client, information from regulated professionals who know the client (lawyers, notaries, accountants, banks) or publicly available information (property registers, company registers, media coverage, internet searches etc.). Examples are listed in the table below:

Provenance of funds to finance the transaction	**Examples of supporting document**
Income from employment	▪ CV with employment history including details of Companys and positions held, or ▪ Information of income from employer, or ▪ Recent accounts if self-employed, or ▪ Bank statements clearly showing receipt of most recent 3 months regular salary payments from named employer, or ▪ Tax return.
Income from business activity	▪ Financial statements or accounts, ▪ Bank statements of the business in question.
Loan	▪ Loan agreement
Property sale	▪ Contract of sale, or ▪ Bank statement showing sale consideration money, or ▪ Letter from accountant, or notary confirming sale, or ▪ Media coverage (if applicable) relating to the sale.
Sale of investments	▪ Certificates, contract notes or statements in the name of the client demonstrating the sale.
Gift	▪ Legal documentation evidencing gift where possible; or ▪ Written statement from the donor confirming the gift.

Inheritance	▪ Legal document providing full details of estate inherited; or ▪ Bank statement if it clearly shows client's full name, address and shows the origin of the funds.
Sale of business	▪ Contract of sale, or ▪ Legal document evidencing sale, or ▪ Media coverage (if applicable) relating to the sale, or ▪ Signed letter from accountant or notary confirming sale.
Compensation payment	▪ Letter from compensating body; or ▪ Court documents setting out details of the claim; or ▪ Legal document evidencing compensation payment.
Return on investments/savings	▪ Certificates, contract notes or statements in the name of the applicant; or ▪ confirmation from the relevant investment company; or ▪ Bank statement showing receipt of funds from the investment company.
Lottery/gambling win	▪ Letter from relevant organisation (Lottery headquarters/betting shop/casino), or ▪ Bank statement showing funds deposited by relevant organisation, or ▪ Media coverage (if applicable) relating to the win.

All information obtained pertaining to the verification of source of funds of a client must be appropriately recorded. Questions asked and answers given by the client and measures taken to verify the information objectively must be documented. The records maintained should enable an independent reviewer such as an investigator to understand how the Company established the source of funds of the client.

Minimum Account Opening

There shall not be any minimum account opening balance since the Company is targeting both retail and institutional clients. There shall also not be any limit in terms of deposit. However, the Company shall ensure that any amount deposited by customers are in line with the customer profile established as part of the CDD process.

With regards to other categories of clients including but not limited to Money managers, financial advisors, institutional, retail and large money managers and similar entities, the Company shall conduct full due diligence exercise on them in accordance with the Customer Due Diligence process highlighted above and verify that they are duly regulated from an AML/CFT perspective by a regulator/authority in a jurisdiction having at least equivalent AML/CFT laws as that of Mauritius. Additionally, in cases where those entities wish to use the platform to manage client portfolios individually (that is accounts are opened in the name of the customers), the Company shall ensure that all such customers are duly identified and have their identity verified in accordance with the Customer Due Diligence process outlined in this Manual, including verification of source of funds.

6.4. Customer AML-CFT risk assessment

In compliance with section 17(1) FIAMLA, based on the identification documents collected and result of screening, an AML-CFT customer risk assessment shall be done. For this purpose a customer risk assessment shall be conducted using the Customer Risk Assessment Tool to determine the level of ML/TF risks associated with doing business with the client.

6.4.1. High risk customers and Enhanced Due Diligence measures

Where a client is categorised as High Risk, for example if the client or its beneficial owner or any of its Principals is a PEP, the Company is required under Regulations 12 and 15 of the FIAMLR, to apply Enhanced Due Diligence measures. Enhanced due diligence (EDD) implies taking additional steps in relation to regular identity verification generally carried out. As laid down under the aforementioned Regulations, EDD measures would entail:

(a) obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of the customer and the beneficial owner;

(b) obtaining additional information on the intended nature of the business relationship;

(c) obtaining information on the source of funds and source of wealth of the customer;

(d) obtaining information on the reasons for intended or performed transactions;

(e) obtaining the approval of the senior management to commence or continue the business relationship;

(f) 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;

For High Risk Clients, approval of the senior management whether to start (if a new client), to continue (in case it is an existing client) or terminate the business relationship will need to be obtained (*refer to Annex 1 for template*). For this purpose complete information regarding availability of identification verification documents, results of screening and EDD documents available will need to be provided to enable an informed decision.

6.4.2. EDD on individual

Where the client is an individual acting in his own name and he is categorised as High Risk customer, for example he is a PEP, or a family member or a close associate of a PEP, the Company shall obtain more information on the source of wealth and other information/documents, including but not limited to obtaining a bank reference issued within the past three months as part of EDD measure. In addition, as long as the business relationship lasts with the client, as an EDD measure, as part of on-going monitoring, the Company shall ensure that the identity verification documents available on the client remain current and valid. For example the passport copy on records has not expired, the proof of address on records is accurate (i.e, address and name of the client has not changed in the meantime). The Company shall also conduct enhanced searches and analysis of the

high-risk factor and same shall be documented on file to further mitigate any risks. Note that the aforementioned measures are not exhaustive and will mainly depend on the type of risk that the customer/prospective customer represent.

Source of wealth and source of funds are two distinct things. Source of wealth is defined as the activity or event which generated the individual's net worth (and not just the funds to be used for the transaction at hand). Source of wealth may also be verified through a combination of sources such as information provided by the client, confirmation from regulated professionals who know the client (lawyers, notaries, accountants, banks) or publicly available information (property registers, company registers, media coverage, internet searches etc.).

A bank reference letter substantiates that (i) the identity and address of the client has been verified by an independent institution, and (ii) that the client is also client of a financial institution regulated for AML-CFT.

The bank reference should be issued on the bank's letterhead and clearly indicate the date on which the letter was issued, the name and title of the bank officer, and contact details of the bank. The bank reference letter ought to state the period for which the individual has been a customer of the bank and confirm that the banking relationship has been acceptable, without any default on the part of the individual. Additionally, the Company shall conduct enhanced searches and document results obtained on the person.

EDD measures will vary depending on the nature of the high-risk posed and there are therefore no tailor-made list of documents which would typically be required.

6.4.3. EDD on Legal person or legal arrangement

When the client is a legal person or legal arrangement, the EDD measure will depend on the reason for which the legal person or legal arrangement has been categorised as High Risk. For example:

- where the client is a legal person and it is categorised as High risk because of the screening result on its shareholder (or equivalent in the legal person or arrangement), or on its beneficial owner, EDD shall be applied by establishing and documenting the source of wealth of the shareholder or beneficial owner in question and any other information that would reasonably be required to document and mitigate the risk;

- where the client is categorised as High risk because of the screening result on its director (or equivalent function in the legal person or arrangement), EDD shall be applied by ensuring that (i) no funds or property from the director in question will be involved in any transaction with the Company and that (ii) the director in question is not the beneficial owner of the legal person. The nature of the high risk posed by the director will also be scrutinized by conducting further searches and analysing the potential ML/TF risks posed;

- in cases where the client is categorised as High risk because of adverse information found on the client itself, EDD shall be applied by obtaining further information to establish the legitimate purpose of the transaction with the Company. The Company

shall also take all reasonable measures to ascertain that its services would not be used for illicit purposes, should it decide to enter into a business relationship with the client.

In the case of new clients being on-boarded, EDD documents must be obtained prior to establishing the relationship with the client. Most importantly EDD documents and/or information must be obtained before accepting any deposit or remittance of funds from the client. If the client has already been on-boarded, EDD documents must be obtained before proceeding further in the transaction.

All information pertaining to EDD conducted on a client must be appropriately recorded. The records maintained should be sufficient to demonstrate to an independent reviewer such as an investigator from the FIU or a competent authority how the Company conducted EDD on the client to ensure that its services are not used for unlawful purposes.

6.4.4. Politically Exposed Persons (PEPs)

Politically Exposed Persons are individuals who are or who have been entrusted with prominent public functions/positions (for example Heads of State or Heads of government, senior politicians, senior government/judicial/ military officials, senior executives of state owned corporations and important political party officials) as well as their relatives and associates.

This includes:-

i. individuals who meet the definition of a PEP in Mauritius (i.e., a domestic PEP),

ii. individuals who meet the definition of a PEP in a foreign country (i.e., a foreign PEP) and

iii. individuals who have been entrusted with a prominent function/position by an international organization, including member of senior management or other functions equivalent to directors, deputy directors and member of the Board of directors (i.e., international organization PEP).

The definition of PEPs would also include family members and close associates of PEPs. Close associates and family members are defined below:

"close associates" —

(a) means an individual who is closely connected to a PEP, either socially or professionally; and

(b) includes any other person as may be specified by a supervisory authority or regulatory body after consultation with the National Committee;

"family members" —

(a) means an individual who is related to a PEP either directly through consanguinity, or through marriage or similar civil forms of partnership; and

(b) includes any other person as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

Identification and Risk Management of PEPs

PEPs present a higher risk from a money laundering and terrorism financing perspective due to the fact that they are more prone to benefit from proceeds of corruption, and also because they can potentially (due to their offices and connections) conceal the proceeds of corruption or other crimes.

PEP may be identified by a number of ways, including but not limited to:

- Screening
- When obtaining information through the CDD process
- By obtaining publicly available information
- By self-declaration of the customer

When a client or beneficial owner has been identified (whether through screening or information available) as being a PEP, in addition to the EDD measures mentioned above, a specific approval from the senior management shall be obtained before establishing or continuing the business relationship using the form enclosed as Annex 1.

Additionally, whenever a customer or a principal of a customer (in case of a legal person or arrangement) is identified as a PEP (by way of reviewing CDD measures received, during the screening process etc), the PEP log (Annex 10) shall be completed accordingly.

6.4.5. Prohibited clients

No business relationship should be established with a client that is categorised as Prohibited following the Customer Risk Assessment. The Company shall immediately cease dealings with the client and a Suspicious Transaction Report shall be filed with the FIU where required. A list of prohibited clients is provided below:

List of prohibited clients (applicable for both individuals and legal persons or legal arrangements)

- Persons identified on Sanction lists (for example United Nations Sanction list[3], or list issued by the National Sanctions Committee) through the screening process;
- Persons whose assets have been frozen under the Dangerous Drugs Act;

[3] The list is available on the website of the FIU and the National Sanctions Secretariat:
http://www.fiumauritius.org/English/United%20Nations%20Security%20Council/2020/Pages/default.aspx
http://nssec.govmu.org/English/unsclist/Pages/default.aspx

- Persons who have been convicted for Money Laundering and/or terrorism financing in Mauritius or overseas;

- Persons who are currently under investigation by a local or foreign authority for charges related to Money Laundering, Terrorism Financing, Corruption, bribery, fraud or any other financial crime.

6.5. Timing of verification of identity, screening and customer risk assessment

Identity verification documents must be requested from the client during the registration phase to subscribe to the Company's services . All reasonable measures need to be taken to obtain all required identity verification documents, conduct screening and perform customer risk assessment prior to establishing the customer relationship and opening of account.

6.5.1. If identity verification documents or EDD documents cannot be obtained

Under Regulation 13 of the FIAML Regulations 2018, no business relationship shall be established/no transaction performed/relationship shall be terminated and a STR must be filed with the FIU if the Company cannot obtain all the information required to establish the identity of the customer.

Under Regulation 12(3) of the FIAML Regulations 2018, the Company is required to terminate the business relationship and file a STR with the FIU where it is unable to perform the required EDD measures. Therefore, an Internal STR shall be made to the MLRO when

1. Identity verification documents cannot be obtained on the client and any of its Principals to its satisfaction (in case the client is a legal person/legal arrangement), and/or
2. EDD measures are required to be applied but the required EDD documents/information cannot be obtained from the customer.

7. CLIENT ACCEPTANCE

Staff members must obtain all necessary information in order to be in a position to complete the risk assessment and rating and to present CDD information to the Compliance Officer for review. The base document that will provide most of this information is the Application Forms, which the Client must complete.

If a prospective Client is risk assessed as Low or Medium Risk then the identification requirements that follow must be presented to the Compliance Officer or MLRO. The Client on-boarding MUST be approved by one director / CEO together with the Compliance Officer or MLRO.

In the event that a prospective Client is risk assessed as High Risk then in addition to these requirements, the Enhanced Due Diligence Requirements, set out below, must be obtained

and presented to the Compliance Officer or MLRO. The Client on- boarding MUST be approved by two directors (which may include the CEO) together with the Compliance Officer or MLRO.

It is at the discretion of the Compliance Officer or MLRO, for a Low-Risk Client to dispense with some of the identification requirements. In the event that staff members do not have all CDD for a Low-Risk potential Client then they should discuss this directly with the Compliance Officer or MLRO.

In cases where not all CDDs received are satisfactory at the time of application, the Compliance Officer or MLRO should determine what level of business can be conducted until satisfactory due diligence documents have been received. Staff members should endeavour to resolve outstanding issues so that only in rare cases will due diligence documents be outstanding for more than 30 days, at which point such delays must be immediately referred to the MLRO for further instruction.

Client acceptance is complete when the due diligence documents have been reviewed and approved by the Compliance Officer or MLRO and the Client is accepted and signed off by the Director(s)/CEO.

7.1 Client Onboarding Process

Request for identity verification documents

Proposed clients registering on the Company's website to use the services of the Company shall, during the registration phase, provide relevant information and submit requested verification documents.

Conduct screening

Once the proposed client has registered on the website of the Company and submitted relevant information and documents, the Onboarding team shall receive the said information and documents and the latter shall proceed with screening.

Conduct Customer Risk Assessment

Following the completion of screening, the Compliance Officer shall proceed to conduct the Customer Risk Assessment using the Customer Risk Assessment Tool designed for this purpose. The identity verification documents and screening reports will need to be taken into consideration when conducting the assessment. If case of a high risk client, EDD measures shall be applied accordingly.

Once the above have been completed, the customer shall be accepted and documents uploaded on the CRM of the Company.

High risk clients

For High risk clients and business relationships involving PEPs, as mentioned earlier Head of Company Approval will need to be obtained. For this purpose he shall take the Customer Risk Assessment into consideration and :-

i. assess the identity verification documents, screening result, Customer Risk assessment and EDD documents obtained on the client,
ii. Take into consideration the proposed services to be provided to the client, and
iii. Make a decision on whether to proceed by signing the document in Annex 1.

8. DEPOSIT CHANNEL

Bearing in mind the money laundering and terrorism financing risks, the Company shall accept deposits from clients only from directly bank account transfer from a bank account held in the name of the client, credit cards/debit cards/prepaid cards in the name of the client and from Paypal. The Company shall not accept deposits from any third party.

Deposits shall be processed via suitable Payment Service Provider(s) ("PSP") which shall provide payment gateway services. In practice, the funds shall be credited to the account of the PSP which shall, upon deduction of the agreed transaction fees, deposits the funds into the client account of the Company for trading activities to take place.

9. ON-GOING MONITORING

In line with Regulation 3 (1) (e) the Company has a legal obligation to conduct ongoing monitoring of a business relationship until the business relationship with a client has ended. The on-going monitoring process shall be conducted on a risk based approach in order to ensure adequate allocation of resources.

9.1 On-going CDD Monitoring

The On-going CDD Monitoring shall be conducted as per the below:

For High-Risk customers – Annually
The ongoing monitoring process shall be conducted annually as from the date of the previous customer risk assessment.

For High-Risk customers:

- Up to date identification documents to be requested from customer and fresh screening conducted prior to conducting another transaction (including accepting another deposit)
- Update customer information such as occupation, and any other relevant information
- Customer Risk Assessment conducted again to re-assess the risks posed by the customer
- Ongoing Monitoring Form (Annex 2) to be completed

- Depending on different aspects (for example on the transaction patterns/activities), further documents may be required from customers
- Assessment of the high risk factors, and enhanced searches/analysis of same

Ongoing CDD Monitoring shall be thereafter conducted every year.

For Low-Risk customers – Every 3 years

The ongoing monitoring process shall be conducted every 3 years as from the date of the previous customer risk assessment.

For Low-Risk customers:

- Up to date identification documents to be requested from customer and fresh screening conducted prior to conducting another transaction (including accepting another deposit)
- Customer Risk Assessment conducted again to re-assess the risks posed by the customer
- Ongoing Monitoring Form (Annex 2) to be completed
- Update customer information such as occupation, and any other relevant information
- Depending on different aspects (for example on the transaction patterns/activities), further documents may be required from customers

Ongoing CDD Monitoring shall be thereafter conducted every 3 years.

Ongoing CDD Monitoring Table

Risk Rating	Frequency of Ongoing Monitoring
Low	Every 3 years
High	Annually

9.2 Transaction Monitoring

Transactions Monitoring is an essential part of the AML/CFT framework in as much as it allows the prompt identification of suspicious transactions. The transaction monitoring process shall be conducted as described below:

Deposit Monitoring

The Company shall monitor deposits made by customers for future trading. In particular, the Company shall have regard to:

(a) Whether the amount being deposited is commensurate with the customer profile

(b) Whether the pattern/frequency of deposits is commensurate with the customer profile and expected deposits

(c) Whether deposits are being made directly from a bank account or credit/debit/prepaid card/Paypal account in the name of the customer

Trades Monitoring

The Company shall ensure adequate monitoring of trading activities of customers on the trading platform. In particular, the Company shall have regard to:

(a) Whether the trading pattern does not appear to have any lawful or economic objectives
(b) Whether the trading pattern does not appear to match the customer profile and any investment objective

Withdrawal/Redemption Monitoring

The Company shall ensure adequate monitoring of any withdrawal/redemption requested by customers. In particular, the Company shall have regard to:

(a) Whether the overall customer activity until withdrawal makes economic sense
(b) Whether the funds requested to be withdrawn are being sent to a bank account or credit card/Paypal account registered in the name of the customer
(c) Whether the withdrawal pattern is commensurate with the customer profile and any investment objective

Screening must be done by running searches on independent and reliable databases using the identity verification documents obtained to ensure that in the meantime (i.e, from the time of initial screening to payment of final deposits) the client or any its Principals (in case the client is a legal person) has not been reported to be:

- a PEP, a family member or close associate of a PEP; or
- Does not have any connections to organized crime, drug trafficking, arms & weapons dealing, human trafficking, foreign official corruption, violent crime, or terrorism; or
- Is or has not been subject to any convictions or allegations of any fraudulent or criminal/questionable activities.

In case screening results irrefutably show that the client or any of its Principals (in case the client is a legal person or legal arrangement):-

- is a PEP, a family member or close associate of a PEPs; or
- has any connections to organized crime, drug trafficking, arms & weapons dealing, human trafficking, foreign official corruption, violent crime, or terrorism; or
- is or has been subject to any convictions or allegations of any fraudulent or criminal/questionable activities,

the Company has a legal obligation to apply EDD meaures. A decision will need to be taken by the Board of Directors (*refer to Annex 1 for template*), whether to continue or terminate the business relationship. For this purpose complete information regarding availability of identification verification documents and results of screening will need to be provided to enable an informed decision.

In case, following the screening it is found that any client or Principals thereof is listed on the United Nations Sanctions List or list issued by the National Sanctions Committee, the Company must **immediately notify** the National Sanctions Secretariat and the FSC, and **submit a STR to the FIU** as detailed in the chapter of this Manual entitled Targeted Financial Sanctions.

Where there are reasonable suspicions that the client may be attempting to use the services of the Company to commit ML/TF an Internal STR must be filed with the MLRO.

9.3 Records of on-going monitoring

All screening reports and Customer Risk Assessment report and Ongoing Monitoring Sheet must be kept and on the respective client's file (whether in hard or soft copy) for the duration of the business relationship and for a period of at least seven years after it ends.

10. TARGETED FINANCIAL SANCTIONS

The United Nations Security Council (UNSC) has imposed sanctions to prevent and counter proliferation and proliferation financing. This includes targeted financial sanctions against specific persons and entities that have been identified as being connected to the proliferation of weapons of mass destruction. All UN member states are required to implement these measures[4].

The UN Sanctions Act was enacted in May 2019 in Mauritius to enable implementation of targeted financial sanctions measures imposed by the UNSC.

Under section 41 of the UN Sanctions Act, the Company must implement internal controls and other procedures to enable it to effectively comply with its obligations under the UN Sanctions Act. These obligations may be categorised as follows:

a) Sanctions screening
    a. Customer Screening
    b. Transaction monitoring
    c. Sanctions Match and Resolving False Positives
b) Reporting obligations

10.1. Sanctions screening obligations

10.1.1 Customer screening

[4] National Sanctions Secretariat. (August 2020). *Guidelines on the Implementation of Targeted Financial Sanctions Under The United Nations (Financial Prohibitions, Arms Embargo And Travel Ban) Sanctions Act 2019*

Section 25 of the UN Sanctions Act requires that, every reporting person must verify whether the details of a listed party match with the particulars of any client, and if so, to identify whether the client owns any funds or other assets in Mauritius. All clients and transactions must therefore be screened against sanctions lists for potential matches.

When establishing a new business relationship, as part of the screening process, the Company shall therefore ascertain whether the prospective client and its Principals (where applicable) are listed on the UN Sanctions List or list issued by the National Sanctions Committee, or if they are connected to persons who are listed on such lists.

The above also applies, when conducting on-going monitoring during the course of the business relationship with a client. Therefore, as part of the screening process for the purpose of on-going monitoring, the Company shall verify whether the client and its Principals (where applicable) are listed on the UN Sanctions List or list issued by the National Sanctions Committee, or if they are connected to persons who are listed on such lists.

10.1.2 Transactions monitoring

Screening against the UN Sanctions List and list issued by the National Sanctions Committee must also be done for each incoming and outgoing transaction before carrying out the transaction on the parties involved in the transaction (i.e., on the remitter, beneficiary, intermediaries and any other party involved in the transaction),

In addition, the following data points must be verified when conducting transaction monitoring:

i. The parties involved in the transaction (i.e., the remitter, beneficiary, intermediaries and other parties involved in the transaction),

ii. Bank names, bank identifier codes and other routing codes, and

iii. Free text fields (such as payment reference/purpose detail).

As mentioned earlier in the Manual pursuant to section 23(1) of the UN Sanctions Act, it is an offence to deal with the funds/other assets of a person listed on the UN Sanctions List or list issued by the National Sanctions Committee established under the UN Sanctions Act.

Section 24 prohibits making funds or other assets or financial or other related services available, directly or indirectly, or wholly or jointly, to or for the benefit of:-

(a) a person listed on UN Sanctions List or list issued by the National Sanctions Committee ;

(b) a party acting on behalf, or at the direction, of a person described under (a) above; or

(c) an entity owned or controlled, directly or indirectly, by a person described under (a) above.

Not complying with section 23 (1) and section 24 is an offence and, on conviction, entails a fine not exceeding 5 million rupees or twice the amount of the value of the funds or other assets, whichever is greater, and imprisonment for a term not less than 3 years.

10.1.3 Sanctions match and resolving false positives

During the screening process if a match is detected (i.e., if it is found that a client, a Principal of a client or a party to a transaction is listed or is connected to a person listed on the UN Sanctions List or list issued by the National Sanctions Committee) the Company must immediately:

1. halt the transaction in question to avoid committing an offence under section 23 of the UN Sanctions Act, and

2. Investigate further based on the information available to the Company and the identifying information provided in the sanctions list to confirm the match.

The Company shall keep a record of false positives that shall be made available to relevant authorities or appropriate third parties (such as the independent AML/CFT auditor and the FSC) upon request.

10.2. Reporting obligations

In case the Company detects a confirmed positive match (i.e., particulars of a client or Principal of a client match the details of a person listed on the UN Sanctions List or list issued by the National Sanctions Committee), the Company is required under section 25(2) of the UN Sanctions Act to make a report to the National Sanctions Secretariat using the template to be downloaded from the website of the National Sanctions Secretariat - http://nssec.govmu.org to the following email address **nssec@govmu.org.**

Failure to report is an offence and on conviction entails a fine not exceeding 5 million rupees and a term of imprisonment not exceeding 10 years.

Where the Company makes a report to the National Sanctions Secretariat under section 25(2), it must also report same to the FSC.

In the event the Company holds, controls or has in its custody or possession any funds or other assets of a person listed on UN Sanctions List or list issued by the National Sanctions Committee, under section 23(4) it must immediately notify the National Sanctions Secretariat of –

(a) details of the funds or other assets in question,

(b) the name and address of the person listed on UN Sanctions List or list issued by the National Sanctions Committee,

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

(i) the name and address of the sender;

(ii) the name and address of the intended recipient;

(iii) the purpose of the attempted transaction;

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

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

The notification must be made using the template to be downloaded from the website of the National Sanctions Secretariat - http://nssec.govmu.org and submitted to the following email address **nssec@govmu.org**

Failure to comply with section 23(4) is an offence and under section 45 of the UN Sanctions Act entails, on conviction, a fine not exceeding 1 million rupees and imprisonment for a term not exceeding 10 years.

Filing of STR

In line with section 39 of the UN Sanctions Act the Company must immediately submit a STR to the FIU if it has any information related to a person listed on UN Sanctions List or list issued by the National Sanctions Committee. Therefore following screening if it is discovered that a client or a Principal of a client is listed on UN Sanctions List or list issued by the National Sanctions Committee, an Internal STR must be submitted to the MLRO of the Company for onward action.

Amendments to UN Sanction List

The UN Sanction list is dynamic and may be amended from time to time, including having additions being made to same. In this event, the FIU shall send a notice to all registered MLRO/DMLRO/Senior Management personnel reporting persons as the case may be. Upon receipt of those notices, the Compliance Officer shall:

(a) Promptly verify whether any of its customers matches with the new addition (an appropriate evidences of such verification shall be kept on records)

(b) Test the screening engine being used by the Company to ensure that their data bases are being promptly updated

11. SUSPICIOUS TRANSACTION REPORTING

Pursuant to section 14 of FIAMLA the Company has a legal obligation to make a report to the FIU as soon as practicable but not later than 5 working days from the day on which it becomes aware of a transaction which it has reason to believe may be a suspicious transaction.

11.1. What is a suspicious transaction?

Section 2 of the FIAMLA defines a suspicious transaction as a transaction which:-
(a) gives rise to a reasonable suspicion that it may involve -
(i) the laundering of money or the proceeds of any crime; or
(ii) funds linked or related to, or to be used for, the financing of terrorism or proliferation financing or any other activities or transaction related to terrorism as specified in the Prevention of Terrorism Act or under any other enactment,
whether or not the funds represent the proceeds of a crime;
(b) is made in circumstances of unusual or unjustified complexity;
(c) appears to have no economic justification or lawful objective;

(d) is made by or on behalf of a person whose identity has not been established to the satisfaction of the person with whom the transaction is made; or
(e) gives rise to suspicion for any other reason.
To note that as per section 2 of FIAMLA, a transaction includes a proposed or an attempted transaction.

Suspicious transactions are transactions for which there are reasonable grounds to suspect they are related to the commission of ML/TF. Reasonable grounds to suspect is determined by what is reasonable taking into consideration the normal business practices and systems within the business operations of the Company and the industry in which it operates. A suspicious transaction may involve several factors that may on their own seem insignificant, but when taken together, may raise suspicion that the transaction is related to the commission or attempted commission of ML/TF[5].

There is no monetary threshold for making a report concerning a suspicious transaction. However, it is an offence under section 5 of FIAMLA to make or accept any payment in cash exceeding 500 000 rupees or an equivalent amount in foreign currency. It is mandatory to report any payment in cash exceeding 500,000 rupees or an equivalent amount in foreign currency.

When two or more transactions totalling 500,000 rupees or the equivalent amount in foreign currency are conducted on behalf of the same client within a short lapse of time, and the Company knows that these transactions or transfers are conducted by, or on behalf of, the same client, they must be treated as a single transaction and be reported to the FIU.

11.2. Indicators of suspicious transactions

The Company should pay attention and ensure prompt identification of any suspicious indicators. Some indicators have been outlined below:

- Not being able to satisfactorily identify the source of fund
- Deposits are being made from sources (for example bank accounts) not in the name of the customer and in the name of an unidentified third party without rationale
- Trading pattern does not appear to have a lawful or economic rationale, and/or is not commensurate with the customer profile
- Cannot obtain up to date CDD information on a customer

11.3. Reporting obligation

[5] Financial Intelligence Unit. (21 January 2014). *Guidance Note 3 Suspicious Transaction Report.*

A STR must be filed with the FIU if the Company cannot obtain all the information required to establish the identity of the client. The Company is required to file a STR with the FIU where it is unable to perform the required EDD measures.

It is the MLRO's responsibility (or that of the DMLRO in his absence) to file STRs to the FIU. No other employee or officer of the Company may file an STR to the FIU. For the MLRO to file STRs to the FIU he needs to be made aware or informed of the suspicious transaction. For this purpose, employees or officers must report suspicious transactions to the MLRO by submitting an Internal STR (*refer to Annex 3 for template*). In the absence of the MLRO, the Deputy MLRO shall have the responsibility of investigating and submitting STRs as applicable.

11.4. When to submit an Internal STR to the MLRO?

An Internal STR (template in Annex 3) shall be made to the MLRO by an employee or officer who comes across the following cases:

- Identity verification documents (during the CDD process) cannot be obtained on the client and any of its Principals (in case the client is a legal person/legal arrangement),
- EDD measure are required to be applied but the required EDD documents cannot be obtained,
- Following Customer Risk Assessment the client is categorised as Prohibited
- Any suspicion that a transaction may be linked to money laundering, terrorism financing or proliferation financing directly or indirectly

Internal STRs may be submitted either in person to the MLRO in a sealed envelope or by sending a PDF attachment by email. Internal STRs and STRs must be treated as strictly confidential.

Once the MLRO / DMLRO receives a STR, he shall acknowledge reception by sending an email to the relevant employee.

a. Tipping Off

Once the employee has made an Internal STR to the MLRO, he should seek guidance from the MLRO on how to deal with the client for/by whom the suspicious transaction is proposed to be or has been made, to avoid alerting the client that the transaction has been reported. Officers and employees of the Company shall not inform or alert the client or any other person that an Internal STR has been made to the MLRO. The MLRO shall be the main point of contact of the Company with the FIU.

The officers and employees of the Company are strictly prohibited from disclosing to any person information or any other matter which is likely to prejudice an investigation on a suspicious transaction. Else, this may constitute an offence (Tipping Off) under the FIAMLA.

Under Section 16(1) FIAMLA the Company and its officers shall not disclose to **any unauthorized person** (including fellow colleagues) that a STR is being or has been filed, or that related information is being or has been requested by, furnished or submitted to

the FIU.) Any person who fails to comply with section 16 (1) shall commit an offence and, on conviction, will be liable to a fine not exceeding 5 million rupees and to imprisonment for a term not exceeding 10 years (section 16(3A) FIAMLA).

b. Handling Internal Suspicious Transaction Reports

As soon as the MLRO receives an Internal STR, he shall make an entry in the STR log (*refer to Annex 4*) along with all the details, and acknowledge receipt by email to the person who submitted the Internal STR.

The MLRO shall be given access to all the relevant information or records to assess whether the transaction is suspicious or not. Following investigation, if the MLRO deems that the transaction is suspicous, he shall submit a STR to the FIU as soon as practicable but not later than 5 working days[6] from the day on which the suspicion arose.

The MLRO shall document the information that was examined to assess the transaction reported and the date the STR was made to the FIU in the STR Log. If the case so warrants, the MLRO shall seek advice from the FIU on how to proceed or handle the client relationship.

If after examination, the MLRO considers that the transaction reported is not suspicious, he shall also document the information that was examined to assess the transaction as well as the reasons for not making a report to the FIU in the STR Log. Documenting the information shall include having a file (physical or electronic) to which only the MLRO or Deputy MLRO shall have access and recording the following documents/information into it:

- Facts which relate to the alleged suspicious activity / transaction
- Documents / evidences / information relating to the internal investigation conducted by the MLRO or Deputy MLRO
- Findings of the internal investigations
- Written minutes of meetings held with employees during the internal investigations (if any)
- Written analysis from the MLRO / Deputy MLRO substentiating the decision to file or not to file a STR to the FIU

Note that the above is a non-exhaustive list.

In a nutshell, the different steps for the MLRO would involve the below when a STR is received from an employee:

- Update the STR log (template in Annex 4) with the date he received the STR, nature and other relevant details;
- Investigate further, including if relevant requesting more documents / information from the client (avoiding tipping off), holding meetings with the employee handling the client etc;
- Deciding on whether to file the STR with the FIU, or not following the investigation; and
- Updating the STR log accordingly.

[6] Saturday, Sunday and Public holidays are excluded from the 5 days.

c. Submission of STR to the FIU

STRs can be submitted to the FIU, either electronically or manually.

i. Electronic submission of STRs

Electronic submission of STRs can be done via the FIU's website[7] (goAML) in the following two manners:

(a) in XML format;

(b) by completing an online web-based STR form on the GoAML platform

To be able to submit STRs via the FIU website, the MLRO/DMLRO must be registered on the GoAML platform with the FIU. Evidence of such registration shall be kept on records.

Once the Company has been registered, verified and accepted by the FIU, the MLRO can submit STRs online.

Registration must be made on the FIU's website through goAML application or on www.mrugoaml.fiumauritius.org by clicking on the Web User Guide for details on registration. Both the MLRO and DMLRO shall be registered as active users on the GoAML platform at all time.

ii. Submission of paper STRs

In the event the Company does not have the technical capability to submit STRs electronically, the MLRO must:

i. download a blank STR form from the FIU's website or by following the link below,:
http://www.fiumauritius.org/English/Reporting/Documents/STR_FORM_FINAL_VERSION.pdf

ii. complete it, and

iii. either have it hand delivered to the reception of the FIU at 10th Floor, SICOM Tower, Wall Street, Ebene Cybercity, Ebene 72201, Republic of Mauritius., or submit it by fax to +230 466 2431.

12. SCREENING AND TRAINING OF EMPLOYEES

12.1. Screening of employees:

It is the Policy of the Company when hiring employees or prior to appointing a director or officer (as defined under the Financial Services Act 2007) to conduct screening on the

[7] http://www.fiumauritius.org/English/Reporting/Pages/default.aspx

candidates to ensure that they are competent and suitable for the position to be fulfilled. Screening measures may include:

(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

Records of screening conducted shall be kept as part of the employment data kept on each employee.

Ongoing Screening

The Company shall adopt an ongoing screening programme to ensure that existing employees do not pose a risk to the Company throughout their employment/engagement time. This may be important to know, for example, if an existing employee has been convicted for any crime, or has been involved in any behaviour that may be detrimental to the Company or its activities. In this context, the below measures shall be applicable for existing employees:

- Conducting a fresh screening on relevant adverse media data bases and UN Sanction list on existing employees every 3 years

12.2. Training of employees:

All employees whose duties relate to the handling of business relationships or transactions should be made aware of the relevant legislation and anti-money laundering and combating financing of terrorism standards. The Company will therefore endeavour to provide training to its officers and employees involved in handling of business relationships or transactions related to the activities of the Company.

Employees shall receive training which shall cover at least:

- Legal obligations of the Company under AML-CFT law, regulations and guidelines;
- the money laundering and terrorist financing vulnerabilities of the products and services offered by the Company;
- The AML-CFT controls and procedures of the Company;
- The identity and responsibilities of the MLRO;
- Identifying and reporting suspicious transactions;
- The criminal sanctions in place for failing to report suspicious transactions;
- New developments including information on current money laundering and terrorist financing techniques, methods, trends and typologies; and
- Information on the changing behaviour and practices amongst money launderers and those of financing terrorism.

New employees involved in the business activities of the Company shall receive AML-CFT awareness training on the measures in place within the Company regarding AML-CFT and their obligation as employee/officer of a financial institution, in accordance with applicable provisions of the law. The new employee shall receive AML-CFT training as soon as reasonably practicable and in any circumstances within one month of the start of employment/contract. The training shall ensure that the new employee/officer is aware of the legal and regulatory obligations placed upon him and enable the new employee to recognise a suspicious transaction and the procedures to be followed in order to adequately report a suspicious transaction.

Additionally, the Company shall provide specific training to members of the board of directors and employee part of senior management. The training shall include:

For the Board of Directors and Senior Management Personnel

- 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.

For the Compliance Officer, MLRO and Deputy MLRO

(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 ML and TF 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.

All training information shall be recorded in the training log (template in Annex 5).

12.2.1. Mandatory attendance at awareness session

As mentioned above, employee awareness sessions are one of the methods chosen by the Company to meet its objective of maintaining or increasing AML-CFT knowledge of employees to enable it to achieve full compliance with its AML-CFT obligations. In addition, employee attendance and performance during awareness sessions/training will be monitored. Therefore, attendance at awareness sessions is compulsory and non-attendance without a reasonable excuse may lead to appropriate disciplinary measures being taken by the Company.

12.3. Compliance Officer, MLRO & Deputy MLRO Training

Since the MLRO/DMLRO are responsible for the proper handling, evaluation and reporting of suspicious transactions to the FIU, they shall be given appropriate training to allow them to fulfil his duties and obligations.

The Compliance Officer is another key employee in as much as he is responsible for the day-to-day oversight of the AML/CFT compliance framework. In this context, it is of utmost importance that the Compliance Officer, the MLRO and DMLRO receives a minimum of 10 hours of training on an annual basis that will focus on his specific role and duties as provided under the FIAML Regulations 2018. This is in accordance with the requirements of the Competency Standards.

13. RECORD KEEPING

13.1. Identity verification and transaction records

Regulation 14 (1) requires the Company, to keep and maintain all records relating to transactions in such a form that permits the prompt reconstruction of each individual transaction.

The Company is required to keep records of all the transactions in which they are involved as well as records of all clients. Accordingly, the Company must be kept:

a) Records relating to the identification of clients and beneficial owners (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents) as well as business correspondence for at least 7 years after the business relationship has ended,

b) Records concerning transactions, both domestic and international, for a period of 7 years after the completion of the transaction

c) Records of all suspicious transaction reports, including accompanying documents

d) Details of all records of all changes made to this Manual in accordance with Section 17A of the FIAMLA 2002.

The Company shall therefore keep the records listed below for a period of at least seven years after the business relationship ends or is terminated on the respective client's file (whether in hard or soft copy):

- Signed terms and conditions
- Identity verification documents (including any EDD) documents, screening results and customer risk assessment done;
- Trading information
- Correspondences relating to the transaction.

In all cases, sufficient information shall be recorded to enable the reconstruction of a transaction with a client.

13.2. Internal and external suspicious transaction reports

In compliance with section 17F of FIAMLA and the AML-CFT Policy of the Company, the MLRO shall keep the following records on the internal suspicious reports received and the STR filed for a period of at least seven years from the date the report was made :

- internal suspicious transactions reports received by the MLRO;
- records of actions taken following receipt of internal suspicious transactions reports;
- records of actions taken to assess whether the transactions reported are suspicious or not;
- records of the information that was examined to assess whether the transactions reported are suspicious or not;
- where after examination the MLRO decided not make a STR to the FIU, a record of the reason for the decision not to make a report to the FIU; and
- all reports made by the MLRO to the FIU.

These records may be kept in soft and/or hard copies.

To note that pursuant to section 13(5) FIAMLA, where a STR has been made to the FIU, the director of the FIU shall, by written notice, require the Company to keep the records in respect of that suspicious transaction for such period as may be specified in the notice.

13.3. Training records

The Company shall maintain records of all AML-CFT trainings delivered to employees as detailed below in the Training Log (*refer to Annex 5 for template*):

- the dates AML-CFT training was provided;
- the nature of the training, including details of contents and mode of delivery;
- the names of the employees who received training; and
- copies of Continuous Professional Development (CPD) records for the Compliance, MLRO and Deputy MLRO.

Changes to Policies and Procedures

The Company shall maintain written records of any changes made to AML/CFT policies and procedures as required under the FIAMLA 2002. This record shall be maintain in a Policy Amendment Log (template in Annex 6)

14. MONITORING & TESTING COMPLIANCE

As provided under Regulation 31 of the FIAMLR, the Company shall have an appropriate policy and procedure for the monitoring and testing of compliance of the Company and activities with its relevant AML-CFT requirements. The monitoring and testing of Compliance level shall include:

- Testing and monitoring as to whether the Company has robust and documented arrangements for managing risks identified by the business risk assessment conducted;
- Prompt actions is taken to remedy any deficiencies identified in terms of AML-CFT

The Testing and monitoring of the Compliance of the Company with the applicable AML-CFT requirements has to be done on an ongoing basis and the exercise should assess the below points:

- the adequacy of its ML/TF risk assessment,
- the adequacy of CDD policies, procedures and processes, and whether they comply with internal requirements,
- the adequacy of its risk-based approach in relation to the services offered clients and geographic locations,
- the training adequacy, including its comprehensiveness, accuracy of materials, training schedule,
- compliance with applicable laws,
- the system's ability to identify unusual activity,
- the adequacy of recordkeeping and
- the review of its Suspicious Transaction Reporting (STR) systems, which should include an evaluation of the research and referral of unusual transaction among others.

The Compliance Officer shall be responsible for conducting the monitoring and testing of compliance with AML/CFT requirements as required under Regulation 31. Furthermore, the results of the monitoring and testing exercise shall be held on records and be reported to the board of directors to ensure that the board has appropriate oversight over the compliance status and effectiveness of AML/CFT control measures implemented.

15. INDEPENDENT AML/CFT AUDIT

In accordance with Regulation 22(1)(d) of the FIAML Regulations 2018, the Company is required to establish an independent audit function to review and verify compliance with and effectiveness of the measures taken in accordance with the FIAMLA and the FIAML Regulations 2018.

15.1 Scope of Audit

As a minimum, the audit exercise should cover the below:

(i) the adequacy of its ML/TF risk assessment,
(ii) the adequacy of CDD policies, procedures and processes, and whether they comply with internal requirements,
(iii) the adequacy of its risk-based approach in relation to the services offered clients and geographic locations,
(iv) the training adequacy, including its comprehensiveness, accuracy of materials, training schedule,
(v) compliance with applicable laws,
(vi) the system's ability to identify unusual activity,
(vii) the adequacy of recordkeeping and
(viii) the review of its Suspicious Transaction Reporting (STR) systems, which should include an evaluation of the research and referral of unusual transaction among others.

15.2 Independence of Auditor

The Audit shall be conducted by an internal or external auditor who is independent of the compliance-monitoring functions and should not be conducted by the Compliance Officer. The auditor can be an employee or an external consultant.

15.3 Outcome of the Audit

Following the audit exercise, an audit report shall be submitted to the attention of the Head of Company by the auditor. The report shall cover the above-mentioned scope, provide observations made pertaining to any deficiency sighted and provide quality recommendations for prompt remedial actions to be taken.

Following receipt of the audit report, an action plan shall be devised to remedy any deficiency observed by the audit within a maximum of one month.

15.4 Frequency of Audit

The independent audit exercise shall be conducted at least every year and all reports shall be kept on records and provided to the FIU upon request. This frequency may be revised by the board of directors depending on the ML/TF risks faced by the Company.

The audit reports shall be submitted to the board of directors for their review, approval and further actions.

16. THIRD PARTY RELIANCE

In accordance with Regulation 21 of the FIAMLR 2018, the Company may rely on a third party to introduce business or to perform the CDD measures on behalf of the Company. In case the Company relies on a third party to introduce business or perform CDD measures on its behalf, the Company shall:

(a) take steps to satisfy himself that copies of identification data and other relevant documentation related to CDD requirements shall be made available from the third party upon request without delay;

(b) satisfy himself that the third party is regulated and supervised or monitored for the purposes of combating money laundering and terrorism financing, and has measures in place for compliance with CDD and record keeping requirements in line with the Act and these regulations.

The Company shall not rely on a third party that is located in a high risk country.

Even where the Company relies on a third party to conduct part or all of the CDD measures on its behalf, the Company shall have prompt access to all the CDD documents which shall be kept on records accordingly.

All steps undertaken under this paragraph (for example the assessment of the regulatory status of the third party) shall be kept on records to be able to demonstrate compliance with Regulation 21 of the FIAMLR 2018.

17. HIGH RISK COUNTRIES

In accordance with Regulation 12(1)(c) of the FIAML Regulations 2018, a reporting person shall apply enhanced CDD measures as describe therein. Furthermore, Regulation 24(1) provides that due consideration shall be given to the below while identifying high risk countries:

(a) strategic deficiencies in the anti-money laundering and combating the financing of terrorism legal and institutional framework, in particular in relation to —

- criminalisation of money laundering and terrorism financing;
- measures relating to CDD;
- requirements relating to record-keeping;
- requirements to report suspicious transactions;
- the availability of accurate and timely information of the beneficial ownership of legal persons and arrangements to competent authorities;

(b) the powers and procedures of the country's competent authorities for the purposes of combating money laundering and terrorist financing including appropriately effective, proportionate and dissuasive sanctions, as well as the country's practice in cooperation and exchange of information with overseas competent authorities;

(c) the effectiveness of the country's system for combating money laundering and terrorism financing in addressing money laundering or terrorist financing risks.

In view of identifying High Risk countries and in accordance with Regulation 24(3) of the FIAML Regulations 2018, the Company shall apply enhanced due diligence measures with regards to all countries identified by the Financial Action Task Force (FATF) on their list of

jurisdictions under increased monitoring. It is noted that the Company shall not entertain any dealings with countries found on the list of jurisdictions for call for actions of the FATF.

Annex 1- Senior Management Approval Form (High-Risk Customers)

Name of Customer	
Date of onboarding (if applicable)	
Risk Rating	High
Reasons for high risk	
Any other comments	

Establishment or continuation of the business relationship is hereby:

Please tick as appropriate

Approved ☐ **Rejected** ☐

Name:

Signature:

Date:

Annex 2-Ongoing Monitoring Form

Please see separately

Annex 3-Internal Suspicious Transaction Report

Internal Suspicious Transaction Report (STR)

Details of business relationship under suspicion

Name of client:

Type of service offered to client:

Date business relationship commenced *(dd/mm/yy)**:***

Details of Suspicion (*please attach relevant documents*)

Suspected Transaction:

Reasons for Suspicion:

*It is an offence to advise the client or any other person of your suspicion and this report. This report must be treated as strictly **CONFIDENTIAL**.*

Reporter's Signature: **Date** (*dd/mm/yy*)**:**

Reporter's name:

FOR MLRO's USE

Date received: **Time**:

Details of Action: (*please attach relevant documents*)

Date assessment completed:

STR submitted to FIU (*please indicate YES/NO*):

Annex 4- Suspicious Transaction Report Log

Internal - Suspicious Transaction Report Log								
Date	**STR filed on (Name of client file)**	**Name of employee filing STR (include position)**	**Reasons for internal STR**	**Received by MLRO or DMLRO**	**MLRO filed STR with FIU (Yes/No)**	**Reasons for filing with FIU (if applicable)**	**Date filed with FIU (if applicable)**	**Feedback from FIU (if applicable)**

Annex 5- Training Log

Please see separately

Annex 6 – Policy Amendment log

Please see separately

Annex 7 – Business Risk Assessment & Methodology

Please see separately

Annex 8 – Customer Risk Assessment & Methodology

Please see separately

Annex 9 – Acknowledgement Form

Please see separately

Annex 10 – Politically Exposed Persons (PEP) Log

Please see separately