COMPLIANCE &
PREVENTION OF MONEY LAUNDERING &
TERRORIST FINANCING MANUAL

December 2024

Review and approved on: 17/12/2024
Review and approved by: Andrey Stoychev (Director)

Signature:……..

Table of Contents

1. DEFINITIONS

(a) **Alternate Compliance Officer** as per the AML Act 2020 means a senior official at management level to act as an alternate compliance officer, with the approval of the supervisory authority in the absence of a compliance officer.

(b) **AML Act** means the Anti-Money Laundering and Countering the Financing of Terrorism Act 2020, which repeals the AML Act 2006 as subsequently amended;

(c) **Benefit from criminal conduct** means any money or property that is derived, obtained or realised, directly or indirectly, by any person from criminal conduct;

(d) **Beneficial owner** as per the Beneficial ownership Act 2020 means one or more natural persons who ultimately own or control a customer or the natural person or persons on whose behalf a transaction is being conducted and includes those natural persons who exercise ultimate effective control over a legal person or a legal arrangement

(e) **Business relationship** means the arrangement between a person and a reporting entity whose primary purpose is to facilitate an occasional or regular course of business dealings between them

(f) **Cash** includes notes and coins of Seychelles or of any other country which is a legal tender and accepted as a medium of exchange in the country of its issue, postal orders, bearer cheques which passes title thereto upon delivery including travelers' cheques, bank drafts and bearer bonds

(g) **Commissioner** means the Commissioner of Police;

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

i. the person in whose name a transaction or account is arranged, opened or undertaken;
ii. a signatory to a transaction or account;
iii. any person to whom a transaction has been assigned or transferred;
iv. any person who is authorised to conduct a transaction; or
v. such other person as may be prescribed;

(i) **Company** means VS Capital Limited which is a company incorporated in Seychelles with Company registration number 8434958-1;

(j) **Compliance Officer (CO)** this is the title of the person that will perform both duties as per provisions of the FSA Act, 2013 and the Anti-Money Laundering Act of 2020

(k) **Criminal conduct** shall have the meaning set out in section 3 of AML Act and includes the financing of terrorism;

(l) **Data** means representations in any form of information or concepts;

(m) **Digital currency or cryptocurrency** means currency that is exclusively stored and transferred electronically, and whose value is determined by the market in which it is traded;

(n) **Financing of terrorism** means any of the offences referred to in sections 5, 6, 7, 8, 9, 10, 12, 15, 16 or 19 of the Prevention of Terrorism Act, 2004;

(o) **FIU** means the unit established under section 10 of the AML Act;

(p) **Law enforcement agency** means the Financial Crime Investigation Unit or any other Unit as may be designated by the Commissioner of Police within the Seychelles Police Force; the Anti-Corruption Commission of Seychelles; the Department of Immigration; the Seychelles Revenue Commission or any other Agency as may be specified by the Minister by notice published in the Gazette to carry out criminal investigation in Seychelles;

(q) **Person** includes a body of persons whether it has legal personality or not;

(r) **Politically Exposed Person** means**:**

1.i. an individual who is or has been, during the preceding three years, entrusted with a prominent public function in:

a. Seychelles;

b. any other country; or

c. an international body or organisation;

ii. an immediate family member of a person referred to in point (1.i); or

iii. a close associate of a person referred to in point (1.i).

2. Politically exposed persons include:

i. heads of state, heads of government, ministers and other and senior politicians;

ii. senior government or judicial officials;

iii. ambassadors and chargés d'affaires;

iv. persons appointed as honorary consuls;

v. high-ranking officers in the armed forces;

vi. members of the boards of central banks;

vii. members of state-owned corporations; and

viii. influential political party officials.

3. Reference to Immediate family members as indicated in section n.1(ii) of a person specified in paragraph n.1(i) above include:

i. a spouse;

ii. a partner, that is an individual considered by his or her national law as equivalent to a spouse;

iii. children and their spouses or partners, as defined in paragraph 3(ii) of this section;

iv. parents; and

v. siblings.

4. Reference to Close associates as indicated in section n.1(iii) of a person specified in paragraph n.1(i) above include:

i. any person who is known to have joint beneficial ownership of a legal person, partnership, trust or any other close business relations with that legal person, partnership or trust; and

ii. any person who has sole beneficial ownership of a legal person, partnership or trust which is known to have been set up for the benefit of that legal person, partnership or trust.

5. In determining whether a person is a close associate of a person specified in paragraph n.1(i) above, a reporting entity shall have regard to public information or such information that the reporting entity has in its possession.

(s) **Prevention of Terrorism Act** means the Seychelles' Prevention of Terrorism Act 2004 as amended;

(t) **Regulated business** means a business for which a license is required under the corresponding Act;;

(u) **Regulatory licence** means a licence specified in the First Schedule of the Anti-Money Laundering Act 2020 as amended;

(v) **Republic** means the Republic of Seychelles;

(w) **Regulations** means the regulations made under the AML Act;

(x) **Suspicious Transactions** means a report on an activity or a transaction or series of transactions made, to be made or attempted to be made, by a reporting entity under section 48 of the AML Act 2020.

2. INTRODUCTION

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

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

This Manual has been prepared in accordance with the provisions of the Anti-Money Laundering Act 2020 (as amended from time to time) and the Prevention of Terrorism Act 2004 (including subsequent Regulations) and in line with internationally recognized principles as well as any code, direction or guideline issued by the Authority as well as the Financial Services Authority Act 2013 (i.e. establishment of Compliance function) as amended from time to time.

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

3. COMPLIANCE FUNCTION

Obligations of the Company under applicable legislation

The Company shall ensure its compliance with the local requirements and its obligations under the Financial Services Authority and the AML Act 2020. In this respect it shall always have appointed an individual approved by the Authority as its Compliance Officer who shall be appointed to oversee the compliance of the Company with (a) section 23 of the Financial Services Authority Act 2013 and section 34 (1) and 34(3) of the AML Act 2020 or any financial services legislation as well as (b) any code, direction or guideline or directives issued by the Seychelles Financial Services Authority that apply to the Company.

As per section 34(3) of the AML Act 2020, the Alternate Compliance Officer shall fulfil the duties of the Compliance Officer in his/her absence.

The Compliance Officer of the Company shall be responsible for:

a. ensuring compliance with laws, regulations and directives;
b. establishing and maintaining a programme for training the staff and other officers of the Company concerning the Company's compliance function, and their individual responsibilities with respect thereto;
c. overseeing the implementation of the internal policies and procedures;
d. to prohibit the realization for the Customers of Company of any operations which may infringe the existing legislation;
e. To decrease the probability of appearance of any problem situations connected with any tax and legal limitations of the Customers of the Company.

The person appointed by the Company to serve as its Compliance Officer for the purpose of Anti-Money Laundering Act may, with the approval of the Authority, be appointed to oversee the Company's compliance function.

Alternate Compliance Officer

The Company shall appoint a senior official at management level as an alternate Compliance Officer, with the approval of the supervisory authority to act in the absence of the Compliance Officer. The alternate Compliance Officer shall be physically present in Seychelles, when acting in the absence of the Compliance Officer. Exemptions may apply in accordance to section 8.2 of the AML Regulations.
The Company shall immediately inform the FSA as soon as the alternative compliance officer assume the functions of compliance officer, for more than five consecutive business days, subject officer to:

a. an alternative compliance officer may assume the functions of CO up to an initial period of 90 days;
b. where the Company needs to extend the term of the alternative compliance officer beyond 90 days, the Company shall request the supervisory authority for an extension with reasonable justification for such extension and specifying the duration of the said extension.

Outsourcing the compliance function (as applicable)

As per the Code of Outsourcing the compliance function that was introduced by the Financial Services Authority, a company is allowed to outsource its compliance function with a service provider, if certain requirements are met by the service provider and the company as well. https://www.fsaseychelles.sc/wp-content/uploads/2020/01/Code-on-Outsourcing-of-Compliance-Function_Final-27012020.pdf

In line with the Section 34(1) of the AML Act, the Company is required to appoint a Compliance Officer who shall be a senior official at management lever or employee with such qualifications and experience as has been prescribed. However, the individual fulfilling the function of Compliance Officer for the purpose of section 23(2) of the FSA Act (i.e. outsourced Compliance Officer) can also be fulfilling the role of the Compliance Officer for the AML Act and be outsourced upon the FSA's approval.

3.1 Basic Principles

The Compliance Officer is responsible for the implementation of laws and directives issued by the Authority. In order for the Compliance Officer to discharge his /her responsibilities properly and independently, the following conditions will be satisfied at all times:

- The Compliance Officer shall be a senior official at management level or employee with such qualifications and experience as may be prescribed and shall be able to respond adequately to the enquiries relating to the Company and conduct of its business;
- The Compliance Officer shall be a resident in Seychelles;
- The Compliance Officer shall be familiar with the provisions of the guidelines that may be issued by the FIU and the relevant supervisory authority;
- The Compliance Officer shall have unrestricted access on demand to all books, records and employees of the Company as may be necessary to fulfil his or her responsibilities;
- The Compliance Officer shall have sufficient seniority to enable him or her, to apply sound and independent judgment; effective interaction with the supervisory authority and senior management regarding the Company's compliance with the established guidelines, policies, laws and practices;
- The Compliance Officer shall have the independence required to objectively perform his or her duties and the Company shall not interfere in any activity that may hinder the independence of the compliance officer;
- be insulated from undue influence from other parts of the business regarding the manner and extent to which he or she is performing the functions and shall have access to the senior management (as appropriate), the Board and the Supervisory Authority to discuss the significant compliance matters.
- The Compliance Officer will be appointed for all compliance functions as described above as well as for any reporting requirement to the Board of Directors and to regulatory authorities.
- The Compliance Officer will not be involved in the performance of services or activities, which monitors.

3.2 Duties and responsibilities of the Compliance Officer

The Compliance Officer will have the following responsibilities:

(a) be responsible for the implementation and on-going compliance of the Company's internal programmes, controls and procedures in relation to its business with the requirements of the AML Act;
(b) be responsible for ensuring that the staff of the Company comply with the provisions of the AML Act and any other law relating to money laundering and terrorist financing activities;
(c) receive and review reports of suspicious transactions, or suspicious activities made by the staff of the Company and, if sufficient basis exists, report the same to the FIU in accordance with the AML Act;
(d) act as liaison officer between the Company, the supervisory authority (i.e. FSA), and the FIU in the matters relating to money laundering, and terrorist financing activities and for compliance with the provisions of the AML Act
(e) participate in all mandatory anti-money laundering and countering the financing of terrorism trainings provided by the FSA;
(f) identify, assess, advise on, monitor and report on the Company's compliance with regulatory requirements and the suitability of its internal procedures on an on-going basis to the Board or senior managers and to the FSA upon request;
(g) ensure that the Company maintains a manual of compliance of the policies, procedures, and systems:
    i. with a compliance framework, which shall be submitted to the FSA for review,upon request;
    ii. with all relevant anti-money laundering and countering the financing of terrorism legal and regulatory obligations of the Company and the processes to allow the staff to report violations confidentially to the CO; and
    iii. to identify the procedures to be followed when there have been breaches or suspected breaches of regulatory requirements or internal policies;
(h) ensure the compliance by staff of the Company with the provisions of the manual of compliance maintained under paragraph (g) and the non-compliance of the provisions of the manual shall be recorded, showing the nature, form and period of non-compliance and such non-compliances shall be made available to the onsite examiners of the FSA, for examination.
(i) develop a compliance culture:
    i. to ensure that all directors and relevant staff are familiar with the laws and regulations of the Seychelles to combat money laundering and terrorist financing activities, which includes an understanding of the relevant compliance policies, procedures and systems of the Company as well and the CO imparts awareness of the need for compliance, thereby developing within the Company a robust compliance culture;
    ii. to monitor the developments and changes in the legislations, policies, standards and other guidelines issued by the international bodies in order to keep the Company updated with the regulatory developments and changes in international requirements;
(j) implement the training programme:
    i. for directors and relevant staff which includes the training programme on general anti-money laundering and countering the financing of terrorism awareness, client acceptance procedures, know your customer (KYC) procedures, remediation and suspicious activity reporting relevant to the Company's activities;
    ii. at least once in every year and whenever there are changes in the laws, regulations or international requirements to ensure that the directors and related staff are aware of the latest developments in the anti-money laundering and countering the financing of terrorism activities;

iii. to undergo additional training, in order to enhance his or her professional skills, at least one in every year;

(k) perform review of the compliance framework and make regular assessment reports to the senior management, identify the deficiencies and making recommendations for any updates or revisions;

(l) ensure the Company conducts self-assessment of its compliance framework and institute any necessary updates or revisions and make available the self-assessment report to the FSA, upon request;

(m) ensure the preparation and submission of an Annual Compliance Report to the FSA authority for information within 90 days after each calendar year (as required).

In addition, the Compliance Officer shall be responsible:

(a) to provide advice and guidance to the employees of the Company on subjects related to Money Laundering and Terrorist Financing;

(b) to maintain a registry with documentation related to the submission, evaluation and escalation of suspicious reports, and all relevant documentation that verify the accomplishment of the Company's and Compliance Officer's duties

(c) Ensuring implementation of the procedures described in the Company's Internal Operations Manual.

(d) Communicating updated copies of Internal Operations manual, internal regulations and of any further instructions and rules that relates to their role and responsibilities in the Company, to all members of staff.

(e) To provide advice and guidance to Company's employees.

(f) Communication with regulatory bodies.

(g) Continuous improvement of the existing control procedures.

(h) Receiving and follow up clients complains/grievances.

(i) Handling of customer complains/grievances.

(j) Reviewing Company's Marketing Communication and checking if has been prepared in accordance with local requirements (i.e. being true and fair).

In the absence of the Compliance officer, the Alternate Compliance Officer will have the above responsibilities when it comes to the duties and responsibilities of the Compliance Officer as per AML Act and Regulations 2020 as amended.

3.3 Handling customers complains or grievances

The Compliance Officer is responsible for handling customers complains or grievances. His duties include the effective and efficient handling of customer's complains or grievances so as to enable the Company to adopt and apply the required actions to prevent the repetition of the same complains or grievances.

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

Complaint handling procedure:

- As a first step the Compliance Officer should review the submitted complaint in order to prevent the repetition of the same complains or grievances.

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

The policy of the Company is to resolve the complaint/grievance within a reasonable time from the date of receipt of the complaint within the timelines indicated in its ***Complaint handling policy***. In case, due to the nature of the complaint/grievanc**e**, more time is required then the Compliance Officer should inform the Client as to the reason why the Company has not been able to resolve the complaint and an estimated time to resolve the issue will be provided.

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

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

3.4 Record keeping procedures

All required by the Law documents/data will be kept either in hard copy or electronic form. The Company will be able to retrieve the relevant documents/data without undue delay and present them at any time to the competent Authority.

Furthermore, the Company will arrange for records to be kept of all services provided and transactions undertaken by it, which shall be sufficient to enable the competent Authority to monitor compliance with the requirements under applicable Laws, the directives issued pursuant to the Law and the More specifically, among others, the following will be kept:

- Copies of documents containing data on contracting parties or their details will be stored for seven (7) years upon completion of a transaction.
- Original or other copies which may be used as proof in criminal, civil and arbitration proceedings, transaction-related documents, and reports will be stored for seven (7) years upon completion of relevant transaction.
- Other documents, including business correspondence will be stored for seven (7) years upon termination of obligations between the Company and contracting parties.

- In case there is an investigation against any customers the documents will be kept according to the instructions of the investigating authority.
- The stored documents will contain information on the following:
    a. The true beneficial owners of the account
    b. The volume of funds or level of transactions flowing through the account
    c. Connected accounts
    d. The origin of the funds
    e. The type and amount of the currency involved
    f. The form in which the funds were placed or withdrawn
    g. The identity of the person undertaking the transaction
    h. The destination of the funds
    i. The form of instructions and authorisation given

Furthermore, the following will be kept:

- Record of services or activities giving rise to detrimental conflict of interest
- "Suspicious Transaction Report", to the FIU
- Requests from FIU
- Employees training records
- Complaint/grievance forms

3.5 General Principles

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

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

Integrity - Conduct business with integrity.

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

Skill, Care and Diligence - Conduct business with all due skill, professional care and diligence and effectively apply internal procedures.

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

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

Obtain information about clients - Obtain adequate information in respect of the Company's clients prior to engaging into any contracts with them.

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

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

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

Conflicts of Interest - Manage conflicts of interest fairly, both between the Company and its customers and between customers themselves.

Insider Trading – Refrain from using any inside information for personal gain.

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

3.6 Qualifications

The Company's Compliance Officer shall be approved by the FSA under section 23 of the FSA and section 34 (1) and 34 (3) only if the Authority is satisfied that the said individual is considered to be fit and proper for this position.

4. DESCRIPTION OF MONEY LAUNDERING AND TERRORIST FINANCING

Money laundering is a process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities. Money laundering enables criminals to maintain control over their illicit proceeds and ultimately to provide legitimate cover for the illegal source of the illicit proceeds. This means that proceeds from criminal activities is converted into assets that gives it an appearance of legitimate money. Money laundering is an international scourge and the failure by the authorities to prevent the laundering of the proceeds of crime will enable criminals to benefit from their illegal activities, thereby making crime a viable proposition. The Financing of Terrorism is defined as an offence established when a person "by means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they will be used in full or in part, in order to carry out a terrorist act or activity". Terrorist financing is a unique form of financial crime. Unlike money laundering, which is finding dirty money that is trying to be hidden; terrorist financing is often clean money being used for lethal purposes.

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

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

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

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

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

<u>Offence of Money Laundering as per AML Act</u>

A person is guilty of money laundering if, knowing or believing that property is or represents the benefit from criminal conduct or being reckless as to whether the property is or represents such benefit, the person, without lawful authority or excuse (the proof of which shall lie on him):

(a) converts, transfers or handles the property, or removes it from the Republic;

(b) conceals or disguises the true nature, source, location, disposition, movement or ownership of the property or any rights with respect to it; or
(c) acquires, possesses or uses the property.

Any person who participates in such conduct as described above is considered to commit the offence of money laundering and shall be liable to be punished accordingly.

The person who commits and found guilty of money laundering is liable on conviction to a fine not exceeding SCR 5,000,000 or to imprisonment for a term not exceeding 15 years or to both; For the same offence a legal person is liable on conviction to a fine not exceeding SCR10,000,000.

5. CORE OBLIGATIONS OF THE COMPANY

The core AML obligations of the Company which are also set out in Part VII of the AML Act and in the Anti-Money Laundering Regulations, 2020 (the AML Regulations) can be summarised as follows:

- To appoint an appropriately qualified and experienced Compliance Officer with responsibility for AML compliance, and to establish and maintain procedures and systems (including an audit function and training programme) sufficient to ensure compliance;
- To apply customer due diligence (CDD) measures, also known as "Know Your Customer" (KYC) measures, using a risk-based approach, in respect of all customers, business relationships and transactions;
- To conduct ongoing monitoring of business relationships, including paying special attention to complex, unusual or large transactions with no apparent economic/lawful purpose, and relationships and transactions with persons in high-risk jurisdictions;
- To stop acting and terminate any existing business relationship whenever unable to apply CDD or ongoing monitoring;
- To maintain records, including records of all prescribed CDD measures and all transactions and related correspondence, for seven years from the transaction or correspondence date or the end of the business relationship;
- To report suspicious transactions or attempted transactions to the FIU; and
- To make disclosures required by the Prevention of Terrorism Act.

All above obligations should be implemented by taking a risk-sensitive approach to due diligence and monitoring by the Company. A different approach might be appropriate to be followed in regards to CDD and ongoing monitoring of customers according to the different risk ratings of those customers. A reporting entity may be allowed to apply *"simplified due diligence"* in certain situations that are deemed to be low-risk for money laundering and financing of terrorism, and required to implement *"enhanced due diligence measures"* in situations that are deemed to be high-risk. The ultimate responsibility of the Company is to identify and address the actual risks arising out of business relationship.

Obligations of the company per the AML Act 2020

a. The Company shall report each transaction that is carried out by or through it involving a cash transaction of SCR 50,000 or more or the equivalent money in the currency of other countries, and retain the details concerning such transactions to the FIU (section 5).
b. The Company shall report each wire transfer that is executed of SCR50,000 or more or the equivalent money in the currency of other countries and retain the details concerning such transactions to the FIU (section 5).
c. The Company is obligated under section 31 to register to the FIU
d. The Company is obligated under section 32 to identify and assess money laundering and terrorist financial risks.
e. The Company is obligated under section 33 to establish and maintain adequate internal control systems and procedures.
f. under section 34 (1) and 34 (3) to appoint a compliance officer and an alternate compliance officer within 30 days of commencement of the Act or commencement of its operations.

6. THE ROLE OF COMPLIANCE OFFICER (CO) UNDER THE AML ACT 2020

The Company must appoint a Compliance Officer with overall responsibility for AML/CFT compliance. The Compliance Officer must be a senior officer who is sufficiently qualified and experienced to comply with the detailed requirements in s 34(1) of the AML Act, to act as the liaison point with the FIU and relevant supervisory authorities in Seychelles, and to command the necessary independence and authority to train and supervise all other officers, employees, and agents within the organisation. As per section 34 (3) of the said Act, the company is also obligated to appoint an Alternate Compliance officer in the absence of the appointed Compliance officer. The said person will be assessed by the competent authorities and deemed to be considered as "fit and proper" for this position.

The Compliance Officer appointed shall:

(a) be a senior official at management level or employee with such qualifications and experience as may be prescribed and shall be able to respond adequately to the enquiries relating to the Company and conduct of its business;
(b) be a resident in Seychelles;
(c) be familiar with the provisions of the guidelines that may be issued by the FIU and the relevant supervisory authority;
(d) have unrestricted access on demand to all books, records and employees of the Company as may be necessary to fulfil his or her responsibilities;
(e) have sufficient seniority to enable him or her, to apply sound and independent judgment; effective interaction with the supervisory authority and senior management regarding the Company's compliance with the established guidelines, policies, laws and practices;
(f) have the independence required to objectively perform his or her duties and the Company shall not interfere in any activity that may hinder the independence of the compliance officer;
(g) be insulated from undue influence from other parts of the business regarding the manner and extent to which he or she is performing the functions and shall have access to the senior management (as appropriate), the Board and the Supervisory Authority to discuss the significant compliance matters.

In addition to the requirements specified above, the Company shall consider the provisions under the First Schedule of the AML Regulations when appointing a Compliance Officer.

It is noted that the Company, if it has not more than five staff members, may apply to FSA to have an individual appointed as the Compliance Officer and in the event of the absence of the appointed Compliance Officer, the Company shall notify the same to the FSA.

The Compliance Officer's specific duties and responsibilities include:

(a) identify, assess, advise on, monitor and report on the reporting Company's compliance with regulatory requirements and the suitability of its internal procedures on an on-going basis to the Board and to the respective supervisory authority.
(b) be responsible for the implementation and on-going compliance of the Company's internal programmes, controls and procedures in relation to its business with the requirements of the AML Act;

(c) be responsible for ensuring that the staff of the Company comply with the provisions of the AML Act and any other law relating to money laundering and terrorist financing activities;

(d) receive and review reports of suspicious transactions, or suspicious activities made by the staff of the Company and, if sufficient basis exists, report the same to the FIU in accordance with the AML Act.;

(e) act as liaison officer between the Company, the supervisory authority (i.e. FSA), and the FIU in the matters relating to money laundering, and terrorist financing activities and for compliance with the provisions of the AML Act

(f) participate in all mandatory anti-money laundering and countering the financing of terrorism trainings provided by the FSA;

(g) identify, assess, advise on, monitor and report on the Company's compliance with regulatory requirements and the suitability of its internal procedures on an on-going basis to the Board or senior managers and to the FSA upon request;

(h) ensure that the Company maintains a manual of compliance of the policies, procedures, and systems, with a compliance framework, which shall be submitted to the FSA for review, upon request; with all relevant anti-money laundering and countering the financing of terrorism legal and regulatory obligations of the Company and the processes to allow the staff to report violations confidentially to the CO; and to identify the procedures to be followed when there have been breaches or suspected breaches of regulatory requirements or internal policies;

(i) ensure the compliance by staff of the Company with the provisions of the manual of compliance maintained under paragraph (h) and the non-compliance of the provisions of the manual shall be recorded, showing the nature, form and period of non-compliance and such non-compliances shall be made available to the onsite examiners of the FSA, for examination.

(j) develop a compliance culture to ensure that all directors and relevant staff are familiar with the laws and regulations of the Seychelles to combat money laundering and terrorist financing activities, which includes an understanding of the relevant compliance policies, procedures and systems of the Company as well and the CO imparts awareness of the need for compliance, thereby developing within the Company a robust compliance culture; and to monitor the developments and changes in the legislations, policies, standards and other guidelines issued by the international bodies in order to keep the Company updated with the regulatory developments and changes in international requirements;

(k) implement the training programme for directors and relevant staff which includes the training programme on general anti-money laundering and countering the financing of terrorism awareness, client acceptance procedures, know your customer (KYC) procedures, remediation and suspicious activity reporting relevant to the Company's activities; at least once in every year and whenever there are changes in the laws, regulations or international requirements to ensure that the directors and related staff are aware of the latest developments in the anti-money laundering and countering the financing of terrorism activities; to undergo additional training, in order to enhance his or her professional skills, at least once in every year;

(l) perform review of the compliance framework and make regular assessment reports to the senior management, identify the deficiencies and making recommendations for any updates or revisions;

(m) ensure the Company conducts self-assessment of its compliance framework and institute any necessary updates or revisions and make available the self-assessment report to the FSA, upon request;

(n) ensure the preparation and submission of an Annual Compliance Report to the FSA authority for information within 90 days after each calendar year.

Furthermore, the Compliance Officer shall ensure that all officers, employees, and agents:

(a) are screened by the Compliance Officer and other appropriate officers before recruitment;
(b) are trained to recognise suspicious transactions and trends and particular risks associated with money laundering and financing of terrorism;
(c) comply with all relevant obligations under AML/CFT laws and with the internal compliance manual.

The Compliance Officer and the Company should perform a review of the procedures and policies that the Company implements and follows on a regular basis so as to ensure that any arrangements are in line with the internal procedures as well as updated in accordance with the applicable AML act and regulations.

Alternate Compliance Officer

The Company shall appoint a senior official at management level as an alternate Compliance Officer, with the approval of the supervisory authority to act in the absence of the Compliance Officer. The alternate Compliance Officer shall be physically present in Seychelles, when acting in the absence of the Compliance Officer.

The Company shall immediately inform the FSA as soon as the alternative compliance officer assume the functions of compliance officer, for more than five consecutive business days, subject to:

(a) an alternative compliance officer may assume the functions of CO up to an initial period of 90 days;
(b) where the Company needs to extend the term of the alternative compliance officer beyond 90 days, the Company shall request the supervisory authority for an extension with reasonable justification for such extension and specifying the duration of the said extension.

As per section 34(3) of the AML Act 2020, the Alternate Compliance Officer shall fulfil the duties of the Compliance Officer in his/her absence.

7. INTERNAL CONTROLS, POLICIES AND PROCEDURES

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

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

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

7.1.1 Risk Based Approach ("RBA")

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

a. Recognises that the money laundering or terrorist financing threat varies across Customers, countries, services and financial instruments;
b. Allows the Company to apply its own approach in the formulation of policies, procedures and controls in response to the Company's particular circumstances and characteristics;
c. Helps to produce a more cost effective system; and
d. Promotes prioritisation of effort and actions of the Company in response to the likelihood of money laundering or terrorist financing occurring through the use of services provided by the Company.

A RBA involves specific measures and procedures in assessing the most cost effective and proportionate way to manage the money laundering and terrorist financing risks faced by the Company. Such measures and procedures include:

a. Identifying and assessing the money laundering and terrorist financing risks emanating from particular Customers, financial instruments, services, and geographical areas of operation of the Company and its Customers;
b. Documenting the policies, measures, procedures and controls to ensure their uniform application across the Company by persons specifically appointed for that purpose;
c. Managing and mitigating the assessed risks through the application of appropriate and effective measures, procedures and controls; and
d. Continuous monitoring and improvements in the effective operation of policies, procedures and controls.

7.1.2 Identification and Evaluation of Risks

The Company shall take measures to identify, assess, understand and monitor its risks of Money Laundering and Terrorist Financing activities and take appropriate measures to mitigate the risks identified.

The Company shall, in identifying and assessing such risks, take into account:

(a) the profile of its customers;
(b) the geographic area in which it conducts business;
(c) the product or products that it deals in;
(d) the service or services that it provides or receives;
(e) the means by which such products or services are delivered;
(f) the transactions that it conducts;
(g) customer due diligence carried out by third parties; and
(h) the technological developments in identifying such risks.

The Company, when assessing the risks of Money Laundering and Terrorist Financing, shall take into account, among others, the outcome of any risk assessment carried out at national level and any regulatory guidance issued by the FIU or a supervisory authority.

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

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

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

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

a. Non-face-to-face customers;
b. Complexity of ownership structure of legal persons;
c. Companies with bearer shares;
d. Companies not resident in Seychelles;
e. Politically Exposed Persons;
f. Customers from high risk countries or from countries known for high level of corruption or organized crime or drug trafficking.

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

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

a. Customer transactions where there is no apparent legal financial/commercial rationale;
b. Situations where the origin of wealth and/or source of funds cannot be easily verified;
c. Unwillingness of Customers to provide information on the Beneficial Owners of a legal person.

- <u>How did the Customer communicate with the Company?</u>

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

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

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

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

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

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

Indicative parameters are the following:

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

7.1.3 Relevant International Organisations

For the implementation of appropriate measures and procedures on a risk based approach, the Compliance Officer ensures that he consults, among others, the recommendations and consultations of the following relevant international organisations:

- Financial Action Task Force (FATF), www.fatf-gafi.org
- Eastern and Southern African Money-Laundering Group
- http://www.esaamlg.org/index.php/methods_trends
- The Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) - www.coe.int/moneyval
- The UN Security Council Sanctions Committees - www.un.org/sc/committees/
- The International Monetary Fund (IMF) – www.imf.org
- FIC (South Africa)- https://www.fic.gov.za
- AUSTRAC – http://www.austrac.gov.au
- FINTRAC- http://www.fintrac-canafe.gc.ca

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

The CDD procedure has the following meaning:

a. identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source. This is related to the electronic verification systems or Digital ID systems that the Company may use for verification of its customers which include among others AML screening and ID verification. These electronic systems are used to conduct CDD and rely upon technology, processes and procedures that provide appropriate level of confidence that the system produces accurate results. They are using credible and reputable open source information to provide accurate data when the Company conducts its CDD procedures and perform checks through these systems. Examples of such open source data include personal information found on:
    i. sanction or watch lists;
    ii. law enforcement, court, regulatory or other government websites;
    iii. political websites and publications such as parliamentary, local government or individual politician websites;
    iv. reputable news media and publications; and
    v. information sources made public by an individual themselves, for example on their website, blog or any social media application.
b. where the customer is not the beneficial owner, identifying the beneficial owner and taking reasonable measures, on a risk-sensitive basis, to verify the identity of the beneficial owner, including, in the case of a legal entity, partnership or trust, measures to understand the ownership and control structure of that legal entity, partnership or trust;
c. obtaining information on the purpose and intended nature of the business relationship and to establish details of the business of the customer or a beneficial owner to enable the reporting entity to identify:
    i. complex or unusual large transactions;
    ii. unusual patterns of transactions which have no apparent economic or visible lawful purpose; or
    iii. any other activity which may be, by its nature, likely to be related to money laundering, financing of terrorism or other criminal conduct; and

d. taking reasonable measures to ascertain the purpose of a one-off transaction and the origin and ultimate destination of funds involved in a one-off transaction or transferred as part of a business relationship.
e. where the customer is not an individual, the reporting entity shall take reasonable measures to:
    i. verify that any person purporting to act on behalf of the customer is authorised to do so, and
    ii. identify and verify the identity of that person.

7.2.1 Obligations for customer identification and due diligence procedures

A. The Company shall carry out customer due diligence measures before establishing a business relationship or carrying out a one-off transaction.

More specifically, the CDD requirements are triggered in the following circumstances:

a. When the Company establishes a business relationship;
b. When the Company carries out every one-off transaction that exceeds SCR 50,000 in cash or through wire transfers, whether in a single or several linked operations;
c. When the Company has doubts about the veracity or adequacy of documents, data or information obtained for the purpose of identification or verification of a customer;
d. When the Company reasonably suspects money laundering, terrorist financing or other serious criminal conduct.

Additionally, the Company shall always apply customer due diligence measures to existing customers at appropriate times on risk-sensitive basis depending on:

a. The type of customer, business relationship, product or transaction; and
b. The guidelines issued by the FIU which are not inconsistent with the AML Act and Regulations.

The Company has also the obligation to be able to demonstrate to its supervisory authority that the extent of the measures is appropriate in view of the risks of money laundering, financing of terrorism or other criminal conduct.

B. Exceptionally the Company may apply the customer due diligence measures during the establishment of a business relationship provided that:
   a. this is necessary so as not to interrupt the normal conduct of business such as:
      i. non-face-to-face business;
      ii. securities transactions; and
   b. there is no reasonably determined and justified suspicion of money laundering, financing of terrorism or other criminal conduct.

The abovementioned exception is clearly permissible only in low-risk cases when necessary to avoid interruption to the normal conduct of business of the Company and in any case the CDD must still be completed as soon as practicable after the establishment of the business relationship. The "as soon as practicable time" for this process can be further determined taking into account specific circumstances, including the nature of the business, the geographical location of the parties as well as whether it is practical to obtain all necessary documents before any other transactions are conducted.

7.2.2 Ongoing Monitoring

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

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

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

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

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

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

7.2.3 Best Industry Practices for Identification/Verification

Below is a list with the minimum steps expected by the Company as good industry practice when establishing a business relationship or preparing for a significant one-off transaction, in order to comply with its CDD obligations and provide a sufficient information base for ongoing monitoring:

1. All identification and verification procedures, including both internal and external communications, should be documented in writing and preserved as records under the AML Act ***for a minimum of seven years*** in a form enabling immediate compliance with any information request from the FIU.

2. The reporting entity should first establish to its satisfaction that it is dealing with a real person (natural or legal) and that any person purporting to act on behalf of a non-individual client or customer is properly authorised to act.

3. Whenever possible, and particularly in the case of a politically exposed person (PEP), the individual that the reporting entity is dealing with should be interviewed personally.

4. The reporting entity should take the necessary steps to identify the beneficial owner or owners of the assets which form the basis of the proposed relationship or transaction, and make appropriate inquiries into the purpose and nature of that relationship or transaction. This may require investigation of corporate ownership and control structures and sources of wealth and/or funds.

5. The reporting entity should then take appropriate steps to verify the identity of (a) the client/customer, (b), if different, the natural person with whom the entity is dealing, and (c), if different, the beneficial owner or owners. Those steps should include checking for alternative names / aliases (s 35 of the AML Act).

6. If the client/customer and/or any beneficial owner is a PEP, the reporting entity shall pay particular attention to the source of wealth and source of funds involved, and obtain prior approval from senior management for establishing a business relationship.

7. The best possible identification documents should be obtained from the prospective client/customer, including properly certified translations of any documents not in English. No single form of identification can be fully guaranteed as genuine or representing correct identity. The identification process will generally need to be cumulative. For practical purposes a person's residential address should be regarded as an essential part of his or her identity.

8. Documents issued by reputable government sources (e.g. identity cards and passports) should be required. Where practicable, copies of the supporting evidence should be retained. Alternatively, reference numbers and other relevant details should be fully recorded.

9. In respect of joint accounts where the surname and/or address of the account holders differ, the identity of all account holders, not only the first named, should normally be verified to ensure that the account is not opened or operated in any fictitious or incorrect name (s 44(1) of the AML Act).

10. Where a client or customer is introduced by a branch or subsidiary of a financial institution located outside Seychelles, provided the identity of the customer has been verified by the introducing branch or subsidiary in line with requirements at least equivalent to those of Seychelles and those identification records are freely and immediately available on request to the reporting entity in Seychelles, it is not necessary for identity to be verified or for the records to be duplicated.

11. Where a prospective client or customer is introduced by an independent intermediary, the reporting entity should determine whether it is entitled to rely on that intermediary to verify the identity of that client/customer on its behalf (r 12 of the AML Regulations) and if so, should establish to its satisfaction that all relevant records kept by the intermediary will be made immediately available to it on request, to enable the reporting entity to comply with its own AML obligations.

12. Where the reporting entity is not able to identify and verify the identity of the prospective client/customer and all relevant beneficial owners in accordance with the AML Regulations, the reporting entity should (a) not establish (or terminate) any business relationship, (b) decline to carry out any transaction, and (c) make an immediate STR to the FIU.

Where business relationships are already established, good industry practice for ongoing monitoring and continuing CDD in accordance with the AML Act requires at least the following steps:

1. The reporting entity should develop and maintain a risk profile for its own business, informed by local and international trends in money laundering and financing of terrorism, which is sufficiently detailed to enable it to identify appropriate areas of focus for transaction monitoring and continuing CDD.

2. Individual client/customer profiles maintained by the reporting entity should include sufficiently detailed information about the nature of the relevant business to enable the early detection of unusual transactions or patterns of transactions and other high-risk activity.

3. All documents, data and information relating to CDD for each client or customer, including alternative names or aliases, should be kept up to date, if necessary by requesting additional or better information from that client/customer or conducting independent inquiries, and regularly reviewed.

4. The reporting entity should have systems in place to ensure that (a) all complex, unusual or large transactions with no apparent economic/lawful purpose, (b) all transactions involving high-risk jurisdictions, and (c) all funds transfers that do not contain complete originator information, are promptly identified and adequately examined, with the findings recorded in writing (s 47 of the AML Act).

All reporting entities which do not operate solely as individuals (including, eg, partners in a law firm) should develop their own manual of compliance procedures, which may involve a number of checks additional to those set out above, and all reporting entities should regularly review their internal arrangements on a risk-sensitive basis. Internal procedures and systems adopted must remain consistent with these guidelines and with the provisions of the law.

7.3 Construction of Economic profile

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

1. The Company must be satisfied that it's dealing with a real person and, for this reason, obtains sufficient evidence of identity to verify that the person is who he claims to be. Furthermore, the Company must verify the identity of the beneficial owners of the Customers' accounts. In the cases of legal persons, the Company obtains adequate data and information so as to understand the ownership and control structure of the Customer. Irrespective of the Customer's type, the Company

requests and obtains sufficient data and information regarding the Customer's business activities and the expected pattern and level of transactions.

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

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

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

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

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

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

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

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

10. Transactions executed for the Customer are compared and evaluated against the anticipated account's turnover, the usual turnover of the activities/operations of the Customer and the data and

information kept for the Customer's economic profile. Significant deviations are investigated and the findings are recorded in the respective Customer's file.

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

7.4 Reliance on third parties for Customer Identification Due Diligence Purposes

The Company may rely on information previously obtained by a third party which covers one or more elements of Customer due diligence. It is provided that, the ultimate responsibility for meeting the above requirements shall remain with the Company.

The Company may rely on the regulated person including a foreign regulated person, if:

a. there is no reasonably determined and justified suspicion of money laundering or terrorist financing activities;
b. information on the identity of each customer and beneficial owner and the purpose and intended nature of the business as per section 35 of the AML Act is provided immediately on opening of the account or commencement of the business relationship; and
c. the Company is satisfied that the regulated person shall:
    i. immediately provide it with the necessary information regarding the identification and independent verification of customer's identity, beneficial owners and the purpose and intended nature of business relationship;
    ii. provide within 3 working days of the request, the copies of identification evidence and other documents relating to the obligation of due diligence;
    iii. be subject to requirements equivalent to those specified under the AML Act and in line with international standards and is supervised for compliance with those requirements in a manner equivalent to those applicable in the Republic; and
    iv. not be prevented by professional privileges or any other restrictions to promptly share information on the customer identification and beneficial ownership information and documentation required.

<u>Assessment of Intermediaries</u>

The Assessment process consist of the following:

a. The Company obtains data and information so as to verify that the regulated third party is subject to professional registration in accordance with the competent law of its country of incorporation and/or operation as well as supervision for the purposes of compliance with the measures for the prevention of money laundering and terrorist financing.
b. The Company must be provided with a written undertaking that the regulated third party applies CDD on an ongoing basis, will keep records of CDD measures for seven years, and will make those records available to the reporting entity without delay on request or if it ceases to carry out business.

7.5 Specific Identification procedures

Considering the AML Act and Regulations, the Company subdivides its CDD procedures and follows different identification procedures according to the category where the client admitted. The Company subdivided its procedures as per below:

7.5.1 Simplified Due Diligence procedure

The Company is permitted to apply "simplified due diligence" in certain situations that are deemed to be low-risk for money laundering and financing of terrorism.

It is worth noting that where there is suspicion of money laundering, financing of terrorism or other criminal conduct, the reporting entity shall apply the following customer due diligence measures instead.

While assessing whether there is a low degree of risk of Money Laundering and Terrorist Financing in a particular situation and the extent to which it is appropriate to apply simplified customer due diligence measures in that situation, the Company shall consider specific risk factors including, among other things:

(a) customer risk factors, including whether the customer is;
   i. a licensed bank which is:
      - subject to the requirements of the domestic legislations to implement the standards set forth by the Financial Action Task Force;
      - supervised for compliance with the requirements under domestic legislations by a regulatory body;
   ii. a recognised foreign bank;
   iii. the Central Bank of Seychelles;
   iv. a public body in Seychelles; or
   v. a legal entity, partnership or trust, the securities of which are listed on a recognised exchange which is licensed under the Securities Act (Cap.208) or in a jurisdiction that is an ordinary member of the International Organisation of Securities Commissions.

(b) product, service, transaction or delivery channel risk factors, including whether;
   i. the product or service is a life insurance policy for which the premium is low;
   ii. the product or service is an insurance policy for a pension scheme which does not provide for an early surrender option, and cannot be used as collateral;
   iii. there are reasonable grounds for believing that the product related to the relevant transaction is a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme;
   iv. it is a product where the risks of money laundering and terrorist financing are managed by other factors such as transparency of ownership.

(c) geographical risk factors, including whether the country where the customer is resident, established or registered or in which it operates is;

i. a country which has effective system to counter the money laundering and terrorist financing activities;
ii. a country identified by credible sources as having a low level of corruption or other criminal activity such as money laundering and the production and supply of illicit drugs; and
iii. a country which, on the basis of credible sources, such as evaluations, detailed assessment reports or published follow-up reports by the Financial Action Task Force, the International Monetary Fund, the World Bank, the Organisation for Economic Cooperation and Development or other international bodies or non-profit organisations:
    - has requirements to counter money laundering and terrorist financing that are consistent with the revised Recommendations set forth by the Financial Action Task Force in February, 2012 and updated from time to time; and
    - effectively implements the said recommendations of the Financial Action Task Force.

The Company may accept Clients who are categorised as low risk Clients and follow the Simplified Due Diligence measures, as applicable.

7.5.2 Customers' Due Diligence measures

Personal customers' resident in Seychelles

The following minimum information should be obtained from prospective customers who are resident in Seychelles:

- true name and any other names used as these are sated on the official identity card or passport;
- correct permanent Seychelles residential address, and postal address if applicable;
- date of birth;
- occupation; and
- source of income and asset base.

Proof of Identification

The true name or names used should be verified by reference to a document obtained from a reputable official source which bears a photograph. A current valid full passport or national identity card, not older than 10 years, should be requested and the number registered. After the Company is satisfied with the proof of ID it keeps copies of the pages containing all relevant information.

Proof of Address

The Company may obtain one of the following documents to verify the Customer's address:

- Requesting sight of a recent (not older than three months) utility bill;
- Telephone bill, bank or other financial institution statement; or
- Insurance policy which includes a residential address (to guard against forged or counterfeit documents care should be taken to check that the document is original);
- Checking an official register such as the electoral roll;
- Checking a current telephone directory; or

- Receiving written confirmation from the person‟ s landlord or employer.

Notes:

- It is not acceptable to use the same verification data or information for verifying the Customer's identity and verifying its home address. Thus separate procedures/documents for Customer's identity and its home address verification are followed.
- An introduction from a respected customer personally known to the manager, or from a trusted member of staff, may assist the verification procedure but ***does not replace the need for address verification***. Details of the introduction should be recorded on the customer's file.

Personal Customers who are not residents in Seychelles

Persons who are not resident in Seychelles and wish to establish business relationships with the Company are subject to verification procedures similar to those for resident customers.

Additionally, the Company may wish to verify identity:

- with a reputable credit or financial institution in the applicant's country of residence; or
- a police character certificate from the applicant‟ s country of residence.

Notes:

- For non-face to face customers (further explanation below) all copies should be certified by notaries, diplomatic officials, or equivalent independent professionals.
- Verification of identity and address should also generally be sought from a reputable credit or financial institution in the applicant's country of residence.
- Steps should be taken to verify the applicant‟ s signature as well.

Companies and other legal entities

In order for a corporate customer to open an account with the Company there is need to identify the beneficial owners and any other persons authorised to act on behalf of the account holder. Furthermore, obtaining information on the purpose and nature of the business relationship, including proof of sources of wealth and initial source of funds, is also important, to enable the Company to conduct ongoing monitoring. Before a business relationship is established with a legal entity, and at appropriate regular intervals after the relationship is established, measures should be taken by way of a company search and/or other commercial enquiries to ensure that the applicant company has not been, or is not in the process of being, dissolved, struck off, wound up or terminated. Further checks should be made whenever the reporting entity becomes aware of changes in the management or ownership structure.

Seychelles companies

The following identification documents shall be obtained:

- The original or a certified copy of the Certificate of Incorporation.

- Memorandum and Articles of Association.
- Business plan.
- Resolution of the board of directors to open an account and confer authority on those who will operate it.
- A search of the file at the Companies Registration Office.

Notes:

- These documents should (but may not always) provide the necessary information on the legal form and control structure of the company, the beneficial owners, powers to bind the entity, the registered address, and other basic particulars.
- Where the company is an International Business Company (IBC) or other special-purpose vehicle, some of this information may not be readily available. Nevertheless, the Company should take all reasonable measures to obtain the required information, either by itself or through an intermediary.
- Evidence that any individual representing the company has the necessary authority to do so should also be sought and retained. In the case of a private company whose directors are not previously known to the Company, the identity of all the directors, all persons authorised to operate the account, and all beneficial owners should be independently verified.
- When signatories to the account change, care should be taken to ensure that the identity of the new signatories has been verified.
- Periodic enquiries to establish whether there have been any changes to directors or shareholders or to the original nature of the business /activity may also be made as necessary.

Non-Seychelles Companies

Where a company is not registered in Seychelles and is not a recognised foreign bank or publicly listed company, the identity of the directors, account signatories, and beneficial owners (if different) should be verified in accordance with the requirements for non-Seychelles personal customers. Enquiries made by the reporting entity should extend as far as practicable to identify those who ultimately own and control the company. Evidence that the individual representing the company has the necessary authority to do so should be sought and retained.

All comparable documents to those listed above for Seychelles companies should be obtained before the account is opened, unless the situation is considered low-risk in which case, within no later than one month of the date of establishing the business relationship, the company should provide:

- certified copies, in English, of its chartered statutes, memorandum and articles or other instrument defining its constitution;
- a list of directors, and also the name and address of a person resident in Seychelles authorised to accept service of any legal process.

Notes:

- If the company is already in existence when the account in Seychelles is opened, the signatures on the mandate should be confirmed by the company's current overseas bankers who should also confirm that they can verify the identity of each signatory. Standards of control vary between

different countries and close attention should be paid to the place of origin of the documents and the background against which they are produced.

Joint accounts

In the cases of joint accounts of two or more persons, the identity of all individuals that hold or have the right to manage the account, are verified according to the procedures for personal customers above.

7.5.3 Normal Risk Clients

Any Client who does not fall under the 'low risk Clients' or 'high risk Clients' categories is to be classified as normal risk in relation to the Money Laundering or Terrorist Financing risk.

The Company may accept Clients who are categorised as normal risk Clients and follow the normal Due Diligence measures as described above.

7.5.4 High Risk Customers and Enhanced Customer Identification and due diligence procedures

When assessing the risks of Money Laundering or Terrorist Financing the Company shall take into account specific risk factors including, amongst others:

(a) Customer risk factors, including whether the:

i. business relationship is conducted in unusual circumstances;
ii. client is a resident or is transacting in a geographical area of higher risk;
iii. client is a legal person or legal arrangement that is a vehicle for holding personal
iv. assets;
v. client or potential client, is a politically exposed person;
vi. client is a company that has nominee shareholders or shares in bearer form;
vii. client is a businesses that are cash-intensive;
viii. corporate structure of the client is unusual or excessively complex given the nature of the company's business;
ix. client is a foreign financial institution or non-bank financial institution;
x. client is a non-profit organization (NPO);
xi. client is a professional service provider;
xii. client is a or is associated with a high net worth individual;

(b) Product, service, transaction or delivery channel risk factors, including whether the:

i. payments are being received from unassociated third parties;
ii. service involves the provision of directorship services or nominee shareholders;
iii. Situation involves non-face-to-face business relationships or transactions, without the necessary safeguards, specified by relevant supervisory authorities through the directions or guidelines;
iv. Situation involves reliance on regulated person under section 42 of the Act;
v. product involves private banking;

vi. product or transaction is one which might favour anonymity;
vii. new products and new business practices are involved, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products;
viii. product or service enables significant volumes of transactions to occur rapidly;
ix. product or service allows the customer to engage in transactions with minimal oversight by the institution;
x. product or service has a high transaction or investment value; and
xi. product or service has unusual complexity;

(c) Geographical risk factors, include:

i. the countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective systems to counter the money laundering or terrorist financing activities;
ii. the countries identified by credible sources such as mutual evaluations, detailed assessment reports or published follow up reports, as having significant levels of corruption or other criminal activity, such as terrorist financing activities, money laundering and the production and supply of illicit drugs;
iii. the countries subject to sanctions, embargos or similar measures issued by the European Union or the United Nations and countries that feature on non-compliant lists (black and grey lists);
iv. the countries providing funding or support for terrorism, or have designated terrorist organisations operating within their country and
v. other countries identified by the reporting entity as higher-risk because of its prior experiences or other factors.

The Company may accept Clients who are categorised as high-risk Clients and follow Enhanced Due Diligence measures, as applicable.

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

Non- face- to -face Customers

Where a Customer has not been physically present for identification process, the Company is obliged to apply equally effective customer due diligence and ongoing monitoring procedures for non-face-to-face customers and to put specific and adequate measures in place to mitigate this higher risk. In such circumstances, the identification process and requests for the establishment of a Business Relationship or an occasional transaction through mail, telephone, the Company must follow:

The established Customer identification and due diligence procedures, as applied for Customers with whom it comes in direct and personal contact and obtain exactly the same identification information and documents.

Additionally, the Company may follow the below good practise measures:

- requiring additional documents;

- requiring certification of documents presented by a notary, diplomatic official, or equivalent independent professional;
- independent contact with the customer;
- third party introduction, where consistent with the AML Regulations regarding reliance on intermediaries to conduct CDD on Company's behalf; and
- requiring an initial payment to be carried through an account in the customer' s name from a banking institution bank subject to equivalent CDD requirements.

Notes:

- The above non-face to face requirements are applied to both natural and legal persons requesting the establishment of a Business Relationship or an occasional transaction through mail, telephone or internet.

Politically exposed person (PEP)

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

A PEP is defined in r 6 of the AML Regulations as an individual entrusted with a prominent public function in the last three (3) years, and includes any immediate family member or close associate of such an individual. It is important to note that both local and foreign PEPs are covered by this definition.

The Company should have a procedure in place to determine if prospective clients and prospective or existing customers are PEPs. That determination is complicated by the fact that the definition of a PEP includes family members and associates thus the Company may rely on public information in determining whether persons are within the definition of "close associates"(for example, partners or joint ventures), and should conduct regular searches and checks for this purpose.

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

Once a PEP is identified, the Company should take the following enhanced measures additionally to the CDD:

a. obtain the approval of the senior management before a business relationship is established with the customer;
b. take adequate measures to establish the source of wealth and source of funds which are involved in the proposed business relationship or one-off transaction;
c. where the business relationship is entered into, conduct enhanced ongoing monitoring of the relationship; or
d. apply such other measures provided for in the guidelines issued by the FIU to compensate for the higher risk of money laundering, financing of terrorism or other criminal conduct.

Accounts in the names of companies whose shares are in bearer form

It is the Company's policy not to accept any companies whose shares are in bearer form or any shell banks.

Trust, nominee, and fiduciary accounts

Where a prospective customer is not the beneficial owner, reporting entities are required by the AML Regulations to take reasonable measures on a risk-sensitive basis to identify the ultimate beneficial owner/s and to verify their identity. An application to open an account or to undertake a transaction by a professional adviser, business or company acting as trustee or nominee:

- Requires satisfactory evidence of the identity of the trustee, nominee, or fiduciary and the nature of their trustee or nominee capacity or duties.
- Where an individual nominee who opens an account on behalf of another is not already known to the financial institution then the identity of that nominee or any other person who will have control of the account should also be verified.
- Enquiries should be made as to the identity of all parties for whom the trustee or nominee is acting and confirmation sought that the source of funds or assets under the trustee's control can be vouched for. If the applicant is unable to supply the information requested, independent enquiries should be made as to the identity of the person who has actual control or for whose ultimate benefit the transaction is undertaken. The results of the enquiries should be recorded in the account opening file.

When the Company establishes a Business Relationship or carries out an occasional transaction with customers falling under this category, it must ascertain the following:

- the legal substance of the trust, nominee or fiduciary account;
- the name and the date of establishment of the relationship,
- the nature of activities of the trust,
- the purpose of establishment of the trust, nominee or fiduciary account;
- the source and origin of funds requesting the relevant extracts from the trust deed, and other related agreements;
- any other relevant information from the trustees.

The Company must also verify the identity of the trustor, the trustee and Beneficial Owners, according to the Customer identification procedures prescribed in the Manual. All relevant data and information should be recorded and kept in the Customer's file.

Notes:

- An application to open an account or undertake a transaction on behalf of an undisclosed third party may be suspicious. Where it is not possible to identify the person(s) for whom or for whose ultimate benefit the transaction is being conducted, for example in respect of foreign trusts where the settlor and beneficiaries cannot be disclosed by the trustees, the account should be profiled as higher-risk and subject to enhanced ongoing monitoring.
- Where money is received by a trust, it is important to ensure that the source of the receipt is properly identified, the nature of the transaction is understood, and where possible confirmation made that

the payments are made only in accordance with the terms of the trust and are properly authorised in writing.

Clubs, associations and charities

Before the establishment of a business relationship with clubs, associations, or charities, the Company should satisfy itself:

- As to the legitimate purpose of the organisation by, for example, requesting sight of the constitution.
- Where there is more than one signatory to a proposed account, the identity of all signatories should be established and verified and, when signatories change, care should be taken to ensure that the identity of the new signatories has been verified.
- Information on the organisation's address and principal owners/controllers should also be collected.

Customers from countries which inadequately apply Financial Action Task Force's recommendations

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

The Company applies the following:

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

In order to implement the above, the Company should take into account:

a. the country assessment reports prepared by the FATF (http://www.fatf-gafi.org);
b. the country assessment reports of other regional bodies that have been established and work on the principles of FATF [e.g. the ESAAMLG (http://www.esaamlg.org/) and the International Monetary Fund (www.imf.org).

Based on the said reports, the Company assesses the risk from transactions and Business Relationships with persons from various countries and decides of the countries that inadequately apply the FATF's recommendations.

One-Off transactions

A one-off transaction means a transaction carried out other than as part of a business relationship that exceeds SCR50,000 in cash or through wire transfers, whether the transaction is carried out in a single operation or several operations which appear to be linked.

Other than the CDD measures, the Company should apply enhanced due diligence to ascertain the purpose/scope of one-off transactions, , as well as the origin and destination of such fund transfers and be extra cautious in the monitoring of Customers performing such transactions for any suspicious activities.

8. RECORD KEEPING

As per sections 47 of the AML Act, the Company is required to maintain records for potential use by the FIU and other agencies in the investigation and prosecution of offences related to money laundering or terrorist financing. The nature of the records that must be maintained:

- Reflects the customer due diligence and ongoing monitoring procedures (CDD) outlined above, and the transactions and other business carried out by the Company.
- All records must be kept **for a period of seven (7) years from** the date of the relevant event or, in the case of an ongoing business relationship, after the business relationship ceases, in a form which is immediately accessible upon request.
- Records do not have to be kept in hard copy. Retention may therefore be by way of original documents, or by way of copies in any machine-readable or electronic form from which a paper copy can be readily produced.
- Electronic records must however be kept in a form that enables appropriate authentication .

Records of CDD procedures

The first category of records that must be maintained is records of all CDD measures applied in respect of the Customers. Every CDD step that is prescribed by the AML Act and Regulations must without limiting the generality of that statement, be reflected in records, including the safeguards required before relying on intermediaries.

Whenever a person's identity has been verified, the records kept by or on behalf of the reporting entity should:

- indicate the nature of the evidence of identity obtained, and
- include either a copy of that evidence, or information sufficient to enable a copy to be obtained without delay.

Transaction and correspondence records

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

Regardless of the form in which the reporting entity chooses to keep them, transaction records must be sufficiently detailed to enable the transaction to be readily reconstructed at any time by the FIU or Attorney General, 47(4) of the AML Act, and, if necessary, to be produced as evidence in criminal proceedings.

Transaction records must adequately identify:

- the nature and date of the transaction;
- the type and amount of currency;
- the type and number of any account with the Company; and
- the name and address of the Company and the responsible officer, employee or agent.

In the case of high-risk transactions, as defined in s 41 of the AML Act, records must also include the written findings produced by the reporting entity after examining the background and purpose of the transaction.

Records of FIU interactions

The third category of records which must be maintained is records of all AML/CFT enquiries received from the FIU and all reports made to the FIU under s 47 of the AML Act (including STRs and responses to information requests.

9. EMPLOYEES' OBLIGATIONS, EDUCATION AND TRAINING

The Company ensures by introducing a complete employee's education and training program that enables all employees to:

a. Understand the systems and procedures in accordance with this Manual;
b. Understand the Laws and Regulations;
c. Recognise and deal with transactions and other activities which may be related to money laundering;
d. Understand the types of activity that may constitute suspicious activity in the context of the business in which an employee is engaged and that may warrant a notification to the Compliance Officer;
e. Understand its arrangements regarding the making of a notification to the Compliance Officer;
f. Be aware of the prevailing techniques, methods and trends in money laundering relevant to the business of the Relevant Person;
g. Understand the roles and responsibilities of employees in combating money laundering; and
h. Understand the relevant findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions of the government of Seychelles other relevant international organisations.

The timing and content of the training provided to the employees of the various departments is adjusted according to the needs of the Company. The frequency of the training can vary depending on the amendments of legal and/or regulatory requirements and employees' duties, however the Company will ensure that the training takes place at least on annual basis.

The training programs aim at educating employees on the latest developments in the prevention of money laundering and terrorist financing, including the practical methods and trends used for this purpose. On-going training is given at regular intervals so as to ensure that the employees are reminded of their duties and responsibilities and kept informed of any new developments.

The Compliance Officer and the Compliance function provides advice and guidance to the employees of the Company on subjects related to money laundering and terrorist financing.

Employees' access to this Manual

The Compliance Officer must ensure that a copy of this Manual is kept at the registered and/or principal office in Seychelles and that it is available to relevant employees to read on a regular basis (at least twice annually). The Compliance Officer must ensure that employees are comfortable with their awareness of legislation and rules which affect them. The Compliance Officer may direct relevant employees to omit sections not relevant to their role and might decide to provide additional training/guidance in respect of certain areas of this Manual.

Furthermore, the Compliance Officer must review this Manual at least annually with a view to ensure it is up to date with the processes of the Company and applicable legislation, monitoring ongoing requirements to amend or enhance this Manual, notifying the employees as necessary.

10. SUSPICIOUS TRANSACTION REPORT (STR)

A. Recognition of Suspicious Transactions/Activities

Reporting entities are required by section 48 of the AML Act to make a suspicious transaction report (STR) in any situation in which the Company:

- has knowledge or reasonable grounds to suspect that any service or transaction may be related, directly or indirectly, to the commission of criminal conduct (as defined in s 3 of the AML Act, including but not limited to money laundering or terrorist financing) or to money or property that is or represents the benefit of criminal conduct;
- has information that may be relevant to an act preparatory to an offence or to money or property that is or represents the benefit of criminal conduct;
- has information that may be relevant to an investigation or prosecution of a person for criminal conduct; or
- has information that may be of assistance in enforcing the AML Act.

The company is also required by section 43(3) of the AML Act to make either an STR or a disclosure under section 34 or 35 the Prevention of Terrorism Act in any situation in which the reporting entity:

- is unable to carry out CDD in accordance with the AML Regulations for any one of its customers; or
- is unable to undertake ongoing monitoring of any business relationship.

Notes:

- It is worth noting that inability to carryout CDD or ongoing monitoring are not dependent on any suspicion of criminal conduct on the part of the customer.
- There may be an obligation to make an STR in the absence of any transaction or proposed transaction.
- It should also be noted that if a reporting entity permits a service or transaction to proceed where the timely making of a STR would have prevented that service or transaction from taking place, that reporting entity is likely to have committed the offence of money laundering.

List of indicators of suspicious activity (not exhaustive)

- To deposit accumulated illegal cash in the banking system or to exchange it for valuable items and thereafter to use the items or funds for legitimate purposes.
- Modern electronic payment systems enable cash to be switched rapidly between 35 accounts in different names and different jurisdictions, making CDD measures particularly difficult to apply.
- The context in which the service or transaction occurs and this will vary depending on the type of business and the nature of the customer. A transaction which is consistent in nature and extent with a customer's known, legitimate business or personal activities or with the normal business profile for that type of account is less likely to be suspicious.

Further examples of suspicious activities can be found in **Annex I**.
A number of recognised general indicators for high-risk transactions for money laundering and terrorist financing, are set out in **Annex II** and useful reference resources for typologies and risk indicators are listed in **Annex III**.

B. Internal Reporting Procedures to the Compliance Officer

Internal Suspicion Report

The Compliance Officer shall receive information from the Company's employees which is considered to be knowledge or suspicion of money laundering or terrorist financing activities or might be related with such activities in a written report form (hereinafter to be referred to as "**Internal Suspicion Report**"), a specimen of such report is attached in the **Annex V.**

Internal Evaluation Report

Once the Compliance Officer receives the Internal Suspicion Report he should then evaluate and examine the information received, by reference to other relevant information and examination of the circumstances of the case with the informer and, where appropriate, with the informer's supervisors. The evaluation of the information is being done on a report (hereinafter to be referred to as "**Internal Evaluation Report**"), a specimen of which is attached in the **Annex VI**.

C. STRs and the role of the Compliance Officer

Where a potentially suspicious transaction or service has been identified by the Company, the Compliance Officer must examine the relevant records to confirm whether there are reasonable grounds to suspect that the service or transaction may be related, directly or indirectly, to the commission of serious criminal conduct (including money laundering or terrorist financing).

It is important to note that although the Compliance Officer has the responsibility to receive and review reports of suspicious transactions made by the staff and if sufficient basis exists, report same to the FIU, should the Compliance Officer not be available an alternate compliance officer appointed as per section 34 subsection (1) and (3) of the AML/CFT Act shall assume the role of reporter for suspicious transactions/activities in the absence of the Compliance Officer.

Where the Company has:

a. knowledge or reasonable grounds to suspect that any service, or transaction may be related to the commission of criminal conduct including an offence of money laundering or of financing of terrorism or to money or property that is or represents the benefit of criminal conduct;

b. information that may be:
    i. relevant to an act preparatory to an offence or to money or property referred to in an offence of money laundering or of financing of terrorism or to money or property that is or represents the benefit of criminal conduct;

ii. relevant to an investigation or prosecution of a person for an offence referred in money laundering or of financing of terrorism or to money or property that is or represents the benefit of criminal conduct;

iii. of assistance in the enforcement of this Act or the Proceeds of Crime (Civil Confiscation) Act, 2008.

If after completing the above review, the Compliance Officer decides that reasonable grounds for suspicion exist, then he/she must immediately proceed to fill out an STR for submission to the FIU. All STRs must be made **within two working days** of ascertaining the reasonable grounds, forming the suspicion, or receiving the information and as set out in **Annex VII**. It is essential that all relevant fields are completed, that the core reason for the suspicion is explained in detail, and that the form is dated and signed or otherwise authenticated.

The STR shall:

a. be in writing and may be given by way of telephone to be followed up in writing, mail, fax or electronic mail or such other manner as may be prescribed;
b. be in such form and contain such details as may be prescribed;
c. be accompanied by relevant supporting documents as listed in **Annex IV;**
d. contain a statement of the grounds on which the reporting entity has the knowledge, holds the suspicion or receives the information; and
e. be signed or otherwise authenticated by the reporting entity.

Notes:

- The knowledge of any officer, employee or agent of the Company is taken to be knowledge of the entity.
- It is essential to ensure: that each relevant employee knows to which person he or she should report suspicions within the institution; and
- That there is a clear reporting chain under which those suspicions are communicated directly to the Compliance Officer, with all necessary supporting documentation, without delay;
- The degree of decision-making responsibility placed on the Compliance Officer is significant. In forming an independent judgement about whether there are reasonable grounds for suspicion, he/she should consider all other relevant information available within the reporting entity concerning the person or business to which the initial report relates;
- When deciding to make an STR, the Company should ensure that funds will not be transferred, or property disposed of or put beyond the reach of the courts of Seychelles. If there is any possibility of these events occurring, the reporting entity should make contact with the FIU by telephone at the earliest opportunity so that appropriate directions can be given to preserve the status quo.
- The company should refrain at all times, under all circumstances, from advising their clients, or the subject(s) of the STR, and about the intention to file or existence of the STR.
- The company is required to maintain records of all STRs made, either in a physical or digital form, for a minimum period of 7 years from the date of the transaction a
- The Company and the supervisory authorities are provided protection under section 54 (3) of the AML/CFT Act for reporting suspicious transactions and activities.

- A compliance officer commits an offence if, they have 'reasonable suspicion' of money laundering activity or criminal property and fail to submit an STR. They will be liable on conviction to imprisonment for a term not exceeding 3 years or a fine not exceeding SCR 400,000, or to both.

The procedure for the submission of suspicious transaction reports (STR's) by the Compliance Officer

Step 1- Identifying suspicious transaction or activity

After detecting a suspicious transaction or activity taking into consideration the indicators in **Annexes I, II and III** and the Compliance Officer decides that reasonable grounds for suspicion exist**,** he/she proceeds to fill out the STR form (**Annex VII)** immediately.

Step 2- How to complete the STR form

The STR needs to create the picture of the suspicious transaction and/or activity as well as the circumstances that gave rise to and support that suspicion. The information provided should be clear and detailed as this will provide a high-quality STR.

Step 3- How to Submit a STR

STR forms must be filed with the FIU in line with section 48 (2) (a) of the AML/ CFT Act and submitted either;

- In writing which will be required to be hand delivered in a sealed envelope and stamped **"CONFIDENTIAL"** addressed to: The Director Financial Intelligence Unit or
- Sent by emailing to the designated email address: suspicious.reporting@fiu.sc.

For security purposes, all completed STRs sent via email must be compressed and encrypted, followed by submission via email, as per the detailed process hereunder:

a) The completed STR form should be compressed into a zipped file (follow the instruction and the video link on the FIU website (www.seychellesfiu.sc) on "How to Compress & Encrypt Using Peazip" for more information on how to compress and encrypt your STR form).
b) Password protect the zipped file before emailing to the FIU;
c) Email only the password-protected zipped file to the same email address, enquiries@fiu.sc;
d) An acknowledgement from FIU, via return email, will be sent which confirms the receipt of the email with the zipped file;
e) After the receipt of the acknowledgement email from the FIU, then in a separate email the person submitting the report is requested to email the password and attach the key file (encryption file) to enquiries@fiu.sc . This is a one-time exercise and the password should be kept securely as the same password will apply every time when reporting to the FIU.

Important note- The steps from a) to e) are only for the first-time reporting. For subsequent reporting, only steps a), b) and c) will need to be performed.

Step 4- Receipt and feedback of STR by the FIU

Within 24 hours of its receipt, the FIU will acknowledge receipt of the STR by sending a signed letter to the disclosing party. During the analysis or investigative process, additional information may be required.

As such, the Company will be required to provide the FIU with any additional information that it holds in relation to the transaction or about the parties to the transaction, if requested to do so.

Step 5- For the instances when an STR is rejected

The FIU will reject STRs which are incomplete, or which do not have sufficient relevant information which will enable them to make an informed determination. The FIU will provide the reason for rejection in a letter. The rejected STR will be treated as a non-reported STR. As such the STR may be re-submitted, once the reason for rejection, informed by the FIU. However, re-submission must be done within **24 hours** of receiving the rejection letter.

Step 6- Record Keeping

The Company is required to maintain records of all STRs made, either in a physical or digital form, for a minimum period of **7 years** from the date of the transaction.

D. Role of the Financial Intelligence Unit (FIU)

The Financial Intelligence Unit (FIU) was established in accordance with AML Act to act as a specialised financial intelligence and assets recovery unit for Seychelles. The FIU has extensively defined statutory objectives, functions, and powers, with core responsibilities including:

a. monitoring, training, and enforcing compliance by reporting entities;
b. investigating criminal conduct; and
c. identifying, restraining, and recovering the proceeds of crime.

All reporting entities are accountable to the FIU for compliance with their AML/CFT obligations. The FIU is responsible for receiving and acting on all suspicious transaction reports (STRs) as explained above, the submission of STRs enables FIU to identify patterns and trends and ultimately detect emerging threats to the financial system. The FIU also has wide-ranging general powers to monitor reporting entities, including powers to inspect business premises and to issue statutory information requests, and can direct individual reporting entities to take any steps necessary to secure compliance with the AML Act.

11. ANNEXES

Annex I – Examples of suspicious activity

Below are some examples of suspicious activity that reporting entities in Seychelles may encounter in the course of conducting business.

A. Suspicious customer behaviour

- Customer is secretive and reluctant to meet in person
- Customer has an unusual, nervous, or excessive demeanour
- Customer is accompanied and watched
- Customer insists that a transaction be done quickly or volunteers the information that a transaction is "clean"
- Customer shows uncommon curiosity or level of knowledge about record keeping or reporting requirements
- Customer attempts to deter compliance with record keeping or reporting duties, through threats or otherwise
- Customer presents inconsistent or confusing details about a transaction or does not appear to understand it
- Customer appears to have only informal records of significant or large volume transactions
- Customer is reluctant to proceed with a transaction after being told it must be reported
- Customer suggests payment of a gratuity or unusual favour
- Transaction or activity involving a politically Exposed Person (PEP)
- Family members or close associates of public officials (PEPs) begin making large transactions not consistent with their known legitimate sources of income
- Transaction or activity differs from the customer’s known or expected activity;
- The purpose or source of funds is ambiguous;

- The customer is nervous or hesitating to provide the information being requested;
- The customer is known to be a subject of an investigation;
- Customer provides false information;
- Customer holds a public position and is conducting an unusual transaction;
- Customer is making payment in cash for substantial amounts.

B. Suspicious customer identification circumstances

- Agent, attorney, or financial advisor acts for another person without proper proof of authority
- Customer is unwilling to provide personal identity information or wants to establish identity using unofficial documents
- Customer furnishes unusual, suspicious, or inconsistent identification documents
- Customer is unusually slow in providing supporting documentation or cannot provide properly certified copies
- Customer spells name differently from one transaction to another, uses alternative names, or uses a consistent address but frequently changes the names of persons involved
- Customer's telephone is disconnected
- Business customer is reluctant to reveal details of business activity or beneficial ownership
- Business customer is reluctant to provide financial statements and other documents or presents documentation noticeably different from those of similar businesses

C. Suspicious indicators relating to terrorist financing and financing of proliferation of weapons of mass destruction

- Account activity of a non-profit organization which is inconsistent with its established purpose
- Transactions involving individuals who are listed on sanction lists or known in the media for having terrorist affiliations
- Transactions involving jurisdictions which are known to be locations where terrorist groups operate
- Customer seems to be using their account from high-risk jurisdictions. Fund raising or donations which are not official, and which do not have a clear

- Individual or entity's online presence supports violent extremism or radicalization
- Customer trades in commodities that may also be dually used in missiles, and chemical, biological and nuclear weapons
- The sudden conversion of financial assets to a virtual currency exchange
- Particulars of the customer or beneficiary of a transaction are similar to those listed under sanctions lists, for example the address, register of directors and shareholder

D. Suspicious employee activity

- Employee exaggerates the credentials, background, financial ability, and/or resources of a customer in internal reporting
- Employee lives a lifestyle that cannot be supported by his/her salary
- Employee frequently overrides internal controls or established approval authority or circumvents policy
- Employee permits or facilitates transactions where the identity of the ultimate beneficiary or counterparty is not disclosed
- Employee avoids taking holidays

Annex II - Indicators of suspicious services and transactions

General Risk Indicators

- Transactions or business relationships with countries known to have weak AML/CFT controls, as narcotic source countries, or countries known for highly secretive banking and corporate laws (high-risk countries), especially if transactions are complex and involve intermediaries
- Transactions, business activity, or frequent international travel not consistent with customer profile or known legitimate sources of income/wealth
- Unusually/unnecessarily complex or "layered" movement of funds
- Transactions involving suspected "shell" entities (corporations with no legitimate reason for existence)
- Large one-off cash transactions without proof of origin of funds
- Frequent and large international money transfers without clear economic reason
- Sudden changes in volume or nature of business activity
- Services or transactions for the benefit of persons suspected to be criminals, or persons related to or closely associated with them
- Uncharacteristically large transactions or deposits by family members or associates of public officials (PEPs)
- Client or customer maintains an inordinately large or complex network of accounts / business entities for the type of business purportedly being conducted
- Business client cannot be identified online or in official registers
- Use of undisclosed intermediaries/agents/nominee

Annex III- Reference sources for AML typologies and risk indicators

- Financial Action Task Force (FATF), *Methods and Trends*
  http://www.fatfgafi.org/publications/methodsandtrends/?hf=10&b=0&s=desc(fatf_releasedate)

- Eastern and Southern African Money-Laundering Group
  http://www.esaamlg.org/index.php/methods_trends

- FIC (South Africa)- https://www.fic.gov.za

- AUSTRAC – http://www.austrac.gov.au

- FINTRAC- http://www.fintrac-canafe.gc.ca

Annex IV – Examples of supporting documents to enclose in the STR

- bank account statements:
- deposit slips;
- published articles;
- photos;
- account opening forms;
- identification documents;
- source of funds;
- swift messages;
- company formation request;
- Business plan; etc...

Annex V: Internal Suspicion Report for Money Laundering and Terrorist Financing

INTERNAL SUSPICION REPORT FOR MONEY LAUNDERING AND TERRORIST FINANCING

INFORMER'S DETAILS

Name: …… Tel: ……...

Department: ……... Fax: ……...

Position: …….

CUSTOMER'S DETAILS

Name: …….....

Address: ……...

…….. Date of Birth: ……

Tel: .....Occupation: ……

Fax: ……...Details of Employer: …….

Passport No: ……. Nationality: ……

ID Card No: ……..... Other ID Details: ……....

INFORMATION/SUSPICION

Brief description of activities/transaction: ……

……..…….

Reason(s) for suspicion: …….

……..

Informer's Signature …… Date ……...

FOR COMPLIANCE OFFICER'S USE

Date Received: ……Time Received: ……Ref……...

Reported to FIU: Yes/NO……. ……Date Reported: ……Ref……

Annex VI: Internal Evaluation Report for Money Laundering and Terrorist Financing

INTERNAL EVALUATION REPORT FOR MONEY LAUNDERING AND TERRORIST FINANCING

Reference: …… Customer's Details: ……

Informer: ……. Department: ……

INQUIRIES UNDERTAKEN (Brief Description)

…….....

…….....

…….....

ATTACHED DOCUMENTS

.....

.....

.....

COMPLIANCE OFFICER'S DECISION

.....

.....

.....

FILE NUMBER.....

COMPLIANCE OFFICER'S SIGNATURE Date

....

Annex VII– Prescribed form for STR

(c) DNFBPs & other non-financial reporting entities

Return AML / CFT/NON-BANKS (ii)

FINANCIAL INTELLIGENCE UNIT

ANTI-MONEY LAUNDERING & TERRORIST FINANCING REPORTING OF SUSPICIOUS TRANSACTIONS

Part 1: Disclosing Party

1. Name of Company ……
2. Address
3. Telephone Number ……
4. Report Related to: ……

Money Laundering ☐

Terrorist Financing ☐

Other Criminal Activities ☐

Part 2: Information on Persor /Entity Engaging in Suspicious Activity or Transactions

1. Full Name of Person or Company ……
2. Date of Incorporation DD/MM/YYYY ……. /……./…….
3. Registered Address ……
4. Operating Address ……

Identification Details of the C ompany Director(s)

A (i) Name ……
A (ii) Date of Birth DD/MM/YYYY ……. /……./…….
A (iii) ID Number ……
A (iv) Passport Number ……
A (v) Nationality
A (vi) Occupation
B (i) Name
B (ii) Date of Birth ……
B (iii) ID Number
B (iv) Passport Number ……

		……
B (v)	Nationality	DD/MM/YYYY ……. /……./…….
B (vi)	Occupation	……
		……
		……
		……

If more than two Company Directors, please fill details in on a separate page

Identification Details of the Beneficial Owner(s)

A (i)	Name	……
A (ii)	Date of Birth	DD/MM/YYYY ……. /……./…….
A (iii)	ID Number	……
A (iv)	Passport Number	……
A (v)	Nationality	……
A (vi)	Occupation	……
A (vii)	Date of Appointment	……
A (viii)	Date of Resignation (if relevant)	DD/MM/YYYY ……. /……./…….
B (i)	Name	DD/MM/YYYY ……. /……./…….
B (ii)	Date of Birth	……
B (iii)	ID Number	DD/MM/YYYY ……. /……./…….
B (iv)	Passport Number	……
B (v)	Nationality	……
B (vi)	Occupation	……
B (vii)	Date of Appointment	……
B (viii)	Date of Resignation (if relevant)	DD/MM/YYYY ……. /……./…….
		DD/MM/YYYY ……./……./…….

If more than two Beneficial Owners, please fill details in on a separate page

Other Known Information Associated Persons/Companies..etc

……
……
……
……
……
……
……
……
……

Part 3: Information about Suspicious Activity or Transaction

1. Date of Transaction — DD/MM/YYYY ……. /……./…….
2. Date of Detection — DD/MM/YYYY ……. /……./…….
3. Amount Involved — ……
4. Currency — ……
5. Type of Transaction

Cash ☐
Swift Transfer ☐
Cheque ☐
Card ☐

6. Full Details and Description of Transaction

……

……

……

……

……

……

7. Reasons why the transaction was reported as suspicious

……

……

……

……

……

……

When submitting this report, please append any additional material that you may consider suitable and which may be of assistance to the Financial Intelligence Unit, i.e. statement, correspondence, vouchers, transfers, account opening and identification documents, etc.

---------- ---------- ----------

Signature of Official **Designation** **Institution's Stamp**

Date: ----------