THAURUS Ltd.
AML Policy

Table of Contents

PART A. LEGISLATIVE AND REGULATORY BACKGROUND 2

1. LEGISLATIVE BASE 2
2. REGULATORY REFERENCES 3
3. INDUSTRY GUIDANCE 4
4. OFFENCES, PENALTIES AND DEFENCES 4
   - *A. Offences and Penalties 4*
   - *B. Defences 10*
5. SANCTIONS REGIME 11

PART B. OVERVIEW AND POLICY FRAMEWORK 11

6. INTRODUCTION 11
7. PURPOSE AND SCOPE 12
8. POLICIES AND PROCEDURES 12
9. PROHIBITED BUSINESS RELATIONSHIPS 13
10. MANAGEMENT AND CONTROLS OF AML RISK 13
11. GOVERNANCE AND CORE RESPONSIBILITIES 15
12. RISK MANAGEMENT FRAMEWORK 17
13. CLIENT ONBOARDING AND ACCEPTANCE 19
14. ONGOING CLIENT MONITORING 21
15. INTERNAL AND EXTERNAL REPORTING 22
16. RECORD RETENTION 23
17. APPENDIX 1. GLOSSARY 24

PART A. LEGAL RULES & REGULATIONS

1. Legislative base

Thaurus Ltd (hereinafter referred to only as the "Company"), as a legal entity, regulated by the Financial Services Commission (FSC) is required to comply with local regulations and follow both, Mauritian legal rules & regulations as well as international standards for the anti-money laundering & combatting the financing of terrorism (hereinafter referred to only as the "AML/CFT") for the purpose of keeping track with the most actual approaches.

Mauritius brought a number of amendments to its AML/CFT framework through the Finance (Miscellaneous Provisions) Act 2018, Act 11 of 2018, which was gazetted on 9 August 2018 in Government Gazette 71 of 2018. The relevant amendments introduced by the Finance (Miscellaneous Provisions) Act 2018 are in force and aim at strengthening the national AML/CFT framework by, inter alia:

(a) enhancing the existing legal framework for preventive measures that apply to financial institutions and Designated Non-Financial Businesses and Professions ("DNFBPs");
(b) extending the scope of the Financial Intelligence and Anti-Money Laundering Act ("FIAMLA") to include proliferation financing;
(c) establishing a legal framework to support the National Risk Assessment exercise;
(d) providing a general penalty for contravention of those provisions of the FIAMLA for which no specific penalty was set out.

In addition, a new set of regulations namely, the Financial Intelligence and Anti-Money Laundering Regulations ("FIAML Regulations 2018") were promulgated on 28 September 2018 and became effective on 01 October 2018. The FIAML Regulations 2018 revoked the Financial Intelligence and Anti-Money Laundering Regulations 2003 and address, inter alia, the following FATF requirements:

(a) Customer due diligence;
(b) Politically exposed persons;
(c) Correspondent banking;
(d) Money or value transfer services;
(e) New technologies;
(f) Wire transfers;
(g) Reliance on third parties; and
(h) Internal control and foreign branches and subsidiaries.

On 21 May 2019, the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 and the Anti-Money Laundering and Combatting the Financing of Terrorism and Proliferation (Miscellaneous Provisions) Act 2019 were enacted and both acts came into operation on the 29 May 2019.

The United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019enables Mauritius to implement the measures under all the United Nations Security Council Resolutions and deal with other matters of international concern, and to give effect to Article 41 of the Charter of the United Nations.

2. Regulatory References

The requirements to prevent and detect money laundering and to counter terrorist financing arise from the FIAMLA and the FIAML Regulations 2018.

3. Industry Guidance

The AML and CFT regulatory requirements are largely pulled together by a set of industry guidance notes, provisions of which the Company aims to incorporate into its policies, procedures, and day-to-day operations.

The Company is adhering to the following guidance documents:

- Financial Action Task Force (FATF) Recommendations that are recognized as the international standard for combating money laundering and the financing of terrorism and proliferation of weapons of mass destruction.
- Any other relevant legislations and general rules and principles issued by IOSCO
- Joint Money Laundering Steering Group (JMLSG) Guidance for the UK Financial Sector Parts I, II, and III, 2017
- FCA's Systems and Controls (SYSC) Rules that require senior management to establish appropriate procedures and controls to implement the requirements of the Money Laundering, Terrorist Financing and Transfer of Funds Regulations (MLR), and to manage the risks of the Company's products and services being used for purposes of financial crime.

4. Offences, Penalties and Defences

A. Offences and Penalties

There are a number of different offences that may be committed under the applicable legislation:

Offence	Penalty/Notes
Section 3 (1) Any person who – (a) engages in a transaction that involves property which is, or in whole or in part directly or indirectly represents, the proceeds of any crime; or	(1) Any person who - (a) commits an offence under this Part; or (b) disposes or otherwise deals with property subject to a forfeiture order under subsection (2), shall, on conviction, be liable to a **fine** not exceeding **2 million rupees** and to **penal servitude** for a term not exceeding **10 years**.
(b) receives, is in possession of, conceals, disguises, transfers, converts, disposes of, removes from or brings into Mauritius any property which is, or in whole or in part directly or indirectly represents, the proceeds of any crime, where he suspects or has reasonable grounds for suspecting that the property is derived or realized, in whole or in part, directly or indirectly from any crime, shall commit an offence. (2) A bank, financial institution, cash dealer or member of a relevant profession or occupation that fails to take such measures as are reasonably necessary to ensure that neither it nor any service offered by it, is capable of being used by a person to commit or to facilitate the commission of a money laundering offence or the financing of terrorism shall commit an offence. (3) In FIAMLA, reference to concealing or disguising property which is, or in whole or in part, directly	(2) Any property belonging to or in the possession or under the control of any person who is convicted of an offence under this Part shall be deemed, unless the contrary is proved, to be derived from a crime and the Court may, in addition to any penalty imposed, order that the property be forfeited.

Offence	Penalty/Notes
or indirectly, represents, the proceeds of any crime, shall include concealing or disguising its true nature, source, location, disposition, movement or ownership of or rights with respect to it. **Section 4** Without prejudice to section 109 of the Criminal Code (Supplementary) Act, any person who agrees with one or more other persons to commit an offence specified in section 3(1) and (2) shall commit an offence. **Section 5** (1) Notwithstanding section 37 of the Bank of Mauritius Act 2004, but subject to subsection (2), any person who makes or accepts any payment in cash in excess of 500,000 rupees or an equivalent amount in foreign currency, or such amount as may be prescribed, shall commit an offence. (2) Subsection (1) shall not apply to an exempt transaction. **Section 8** (1) Any person who – (a) commits an offence under this Part; or (b) disposes or otherwise deals with property subject to a forfeiture order under subsection (2), shall, on conviction, be liable to a fine not exceeding 2 million rupees and to penal servitude for a term not exceeding 10 years.	

Offence	Penalty/Notes
(2) Any property belonging to or in the possession or under the control of any person who is convicted of an offence under this Part shall be deemed, unless the contrary is proved, to be derived from a crime and the Court may, in addition to any penalty imposed, order that the property be forfeited. (3) Sections 150, 151 and Part X of the Criminal Procedure Act and the Probation of Offenders Act shall not apply to a conviction under this Part.	
Section 16: Tipping-off No person directly or indirectly involved in the reporting of a suspicious transaction under this Part shall inform any person involved in the transaction or to an unauthorized third party that the transaction has been reported or that information has been supplied to the FIU pursuant to a request made under section 13(2) or (3).	Any person who fails to comply with subsection (1) shall commit an offence and shall, on conviction, be liable to a **fine** not exceeding **5 million rupees** and to **imprisonment** for a term not exceeding **10 years**.
Section 17(C): Customer due diligence requirements Any person who knowingly provides any false or misleading information to a reporting person in connection with CDD requirements under the FIAMLA or any guidelines issued under this Act shall commit an offence and shall, on conviction, be liable to a fine not exceeding 500, 000 rupees and to imprisonment for a term not exceeding 5 years.	**Fine** not exceeding **500,000 rupees** and to **imprisonment** for a term not exceeding **5 years**.

Offence	Penalty/Notes
Section 19: Offences relating to obligation to report and keep records and to disclosure of information prejudicial to a request Offences relating to obligation to report and keep records and to disclosure of Information prejudicial to a request (1) Any bank, cash dealer, financial institution or member of a relevant profession or occupation or any director, employee, agent or other legal representative thereof, who, knowingly or without reasonable excuse – (a) fails to – i. supply any any information requested by the FIU under section 13(2) or 13(3) within the date specified in the request; ii. make a report under section 14; or iii. any person who fails to comply with sections 17 to 17G shall commit an offence and shall, on conviction, be liable to a fine not exceeding 10 million rupees and to imprisonment for a term not exceeding 5 years. (b) destroys or removes any record, register or document which is required under FIAMLA or any regulations; (c) facilitates or permits the performance under a false identity of any transaction falling within this Part, shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years. (2) Any person who – (a) falsifies, conceals, destroys or otherwise disposes of or causes or permits the falsification,	**Fine** not exceeding **10 million rupees** and to **imprisonment** for a term not exceeding **5 years.** **Fine** not exceeding **one million rupees** and to **imprisonment** for a term not exceeding **5 years.**

Offence	Penalty/Notes
concealment, destruction or disposal of any information, document or material which is or is likely to be relevant to a request to under the Mutual Assistance in Criminal and Related Matters Act 2003; or (b) knowing or suspecting that an investigation into a money laundering offence has been or is about to be conducted, divulges that fact or other information to another person whereby the making or execution of a request to under the Mutual Assistance in Criminal and Related Matters Act 2003 is likely to be prejudiced, shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years. **Section 19E: Duty to provide information for purpose of conducting risk assessment** Any person who fails to comply with a request made under subsection (2)(b) shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.	**Fine** not exceeding **one million rupees** and to **imprisonment** for a term not exceeding **5 years.** **Fine** not exceeding **one million rupees** and to **imprisonment** for a term not exceeding **5 years.**

All employees should note that:

- all the offences listed above are criminal offences and committing them is punishable by prison sentences and/or a fine;
- offences can be committed by employees as individuals even if they are acting in the course of their employment;

- in addition to the criminal offences as noted above, any failure to follow the Policy by the relevant employee may lead to disciplinary action being taken at the discretion of the Company's management.

B. Defences

There are certain defences available for some of the offences listed above. The main defence relevant to the Company's employees is the defence of having made an 'authorized disclosure', which is a disclosure made:

- before an offence is committed;
- while it is being committed but an employee started the act at a time when, because he did not know or suspect that the property constituted or represented a person's benefit from criminal conduct, the act was not an offence, and the disclosure is made on the employee's own initiative and as soon as is practicable to make it;
- after the offence was committed, but there is a good reason for the employee's failure to make the disclosure before the act was done, and the disclosure is made on the employee's own initiative and as soon as it is practicable to make it.

If an employee makes a disclosure to the MLRO in accordance with the Procedure for Internal Suspicious Activity Reporting as specified in the AML Manual, then that disclosure will be sufficient for the employee to rely on this defence, provided a disclosure is made before any offence has been committed. This is why it is so important for all employees to read this Policy carefully, comply with its requirements and act quickly.

The MLRO will then decide whether to report the suspicion to the Financial Intelligence Unit (FIU).

If the MLRO submits suspicious activity report to the FIU, an employee must discuss with the MLRO what information can be given to the client, so that this does not result in an offence of tipping off.

5. Sanctions Regime

There is a separate but related sanctions regime that imposes restrictions on the Company's ability to do business with those persons and entities on UN and European Union sanctions lists. Some entries on the lists are specific to a particular person or entity and others are general financial sanctions on all persons and entities in a particular jurisdiction. Screening of all clients against sanctions lists in Risk Screening Tool (the Company is discussing to contract World Check from the company Refinitiv or Membercheck) as an integral part of the Company's KYC and Client Due Diligence procedures, and is done within (1) onboarding of a new client, and (2) during ongoing monitoring on a regular basis, following the risk assessment of clients (the higher the risk, the more frequent regular checks). The Company's Client Acceptance Policy (CAP) stipulates that application from a client, where he is identified as true match on sanction list during KYC procedure, shall be rejected and no business activity shall be initiated with such client.

PART B. OVERVIEW AND POLICY FRAMEWORK

6. Introduction

It is of critical importance for the Company's integrity and reputation, to be able to identify, report, and take precautions to guard against money laundering and financing of terrorism. The nature of the Company's business requires it to abide by anti-money laundering (AML) and countering the financing of terrorism (CFT) legislation and regulation that apply to the trading activities. In addition, the Company may be particularly attractive to individuals seeking to clean-up money due to non-face-to-face nature of the services.

In order to prevent the criminals from using the Company's products and services for laundering the proceeds of crime, it is required to establish appropriate and proportionate to the level of risk, systems and controls, and ensure their effective implementation. Therefore, this Policy is designed to ensure that the Company has a defined and approved by senior management overarching framework to comply with all applicable anti-money laundering and countering the financing of terrorism legislation and regulations.

The Policy is supplemented by Operating Procedures Manual and other Associated Policies and Proceduresdesigned to ensure AML & CFT compliance during the day-to-day operations of the Company.

7. Purpose and Scope

The principal objectives of this Policy are to:

- prevent the Company from being used by money launderers to further their illicit business;
- define a framework to enable the Company to assist law enforcement agencies in identifying and tracking down money launderers and their criminal property;
- ensure that the Company remains compliant with all relevant anti-money laundering, CFT and sanctions legislation and regulations;
- inform all relevant employees about the obligations of the Company and their obligations in relation to complying with AML & CFT laws and regulations.

This Policy applies to all employees of the Company, its vendors, partners, and any external parties involved in client referral, client onboarding and transaction processing.

8. Policies and Procedures

Thaurus is committed to the highest standards of Anti-Money Laundering (AML). The members of the Management Board and all employees are required to adhere to these standards to protect Thaurus and its reputation from being misused for money laundering and/or terrorist financing or other illegal purposes.

Company will examine its AML and AFC strategies, goals and objectives on an ongoing basis and maintain an effective program.

Company has implemented clear rules and regulations into in the AML and operations procedure manuals and which must be complied with by all Company's staff and implemented into day-to-day business. All policies and policy-related documents are published on a global policy platform so they can be accessed by all staff at any time. They are subject to an annual review cycle to ensure their conformity with AML regulations.

9. Prohibited Business Relationships

Company must refuse to open an account/enter into a relationship or has to close an existing account/terminate a relationship, if the company cannot form a reasonable belief that it knows the true identity of the client and/or UBOs and/or the nature of business or formal requirements concerning the identification of the client and/or UBOs are not met. In particular, the company will not

a) Accept assets that are known or suspected to be the proceeds of criminal activity
b) Enter into/maintain business relationships with individuals or entities known or suspected to be a terrorist or a criminal organisation or member of such or listed on sanction lists
c) Maintain anonymous accounts, accounts for shell banks or pay-through accounts
d) Enter into relationships with clients operating in prohibited industries

10. Management and Controls of AML Risk

Company maintains a comprehensive set of measures to identify, manage and control its AML risk. These measures are

a) Controls
b) KYC program

c) A training and awareness program for Company's staff

d) Processes to ensure staff reliability

a) Controls

Adherence to the group-wide AML/AFC program needs to be reviewed regularly to ensure that the Company's efforts are successful. The Compliance Manager/AML Officer is obliged to conduct appropriate controls.

b) KYC Program

Company has implemented a strict KYC program to ensure all kinds of customers (natural or legal persons or legal structures, correspondent banks) are subject to adequate identification, risk rating and monitoring measures. This program has been implemented globally and throughout all business divisions

KYC includes not only knowing the clients and entities the Bank deals with (either as a single transaction or ongoing relationship), or renders services to, but also the Ultimate Beneficial Owners (UBOs), Legal Representatives and Authorised Signatories as appropriate.

The program includes strict identification requirements, name screening procedures and the ongoing monitoring and regular review of all existing business relationships.

Special safeguards are implemented for business relationships with politically exposed persons (PEPs) and clients from countries or industries deemed high risk.

c) Training Program

Company implements a comprehensive AML/AFC training program to ensure that all staff, in particular individuals responsible for transaction processing and/or initiating and/or establishing business relationships, undergo AML awareness training.

The training is tailored to the business to ensure that staff are aware of different possible patterns and techniques of money laundering which may occur in their everyday business. Training also covers the general duties arising from applicable external (legal and regulatory), internal requirements and the resulting individual duties which must be adhered to in everyday business as well as typologies to recognise money laundering or financial crime activities.

11. Governance and Core Responsibilities

The Policy is part of the Company's risk management framework, alongside its arrangements for assessing and mitigating risks (including financial crime risks), senior management's formalized roles and responsibilities, regular reporting to the board, Operating Procedures Manual, employee training and awareness arrangements. These arrangements are collectively designed to ensure that the Company:

- conducts its business in line with the law and proper standards;
- pro-actively identifies and prevents financial crime risks it is exposed to.

(1) The Board of Directors:

- reviews the financial crime policies and procedures, suggest changes and approves them;
- reviews regular financial crime reports and annual report prepared by Money Laundering Compliance Officer;
- reviews the adequacy and effectiveness of the AML & CFT systems and controls employed;

- ensure that the Company complies with its obligations under the legislation;
- address any issues raised by the regulators and define the action to be taken in case corective measures are required;
- update job titles and roles.

(2) MLRO[1] is responsible for:

- appointing the Compliance Officer, and providing direction to, and oversight of the Company's AML & CFT strategy;
- commissioning at least annually a report from the Compliance Officer on the operation and effectiveness of the firm's systems and controls to combat money laundering and terrorist financing, and taking any necessary action to remedy deficiencies identified by the report in a timely manner;
- reviewing the performance of the Compliance Officer;
- establishing and updating appropriate policies, controls and procedures to mitigate and manage effectively the risks of money laundering and terrorist financing;
- ensuring AML & CFT Policies and Procedures are kept up-to-date;
- overseeing the development and reviewing all financial crime and compliance policies including AML & CFT Policy;
- monitoring compliance with all relevant laws, regulations and policies and reporting any material or relevant non-compliance to the Board of Directors.

(3) Compliance Officer:

- oversees the Company's compliance with the rules on systems and controls against money laundering;

[1] Whenever this responsibility is shared, the annual Compliance Officer report and Compliance Officer performance is to be reviewed by the higher standing senior manager.

- ensures the establishment and maintenance of adequate and effective AML & CFT risk management systems and controls;
- monitors day-to-day compliance with the AML & CFT policies and procedures;
- acts as the focal point for all issues related to ML and TF and primary interface with the regulatory authorities and law enforcement agencies.

The senior managers' prescribed responsibilities and key responsibilities are formalized in the Company's Senior Management Structure, Roles & Responsibilities Statement.

All relevant[2] employees are required at all times to comply with this Policy, associated AML Manual and Operational guidelines. Non-compliance by employees with these policies and procedures may be considered as gross misconduct and could result in a disciplinary offence which could lead to dismissal and depending on the nature of the issue, the employee will possibly be subjected to criminal proceedings.

12. Risk Management Framework

To facilitate and ensure compliance with AML & CFT laws and regulations and sanctions regime, the Company is actively implementing a set of measures, consisting of policies, procedures, internal systems

and controls. The development and implementation of such adequate measures and their effectiveness, is managed and overseen by the Company's senior management. These measures are applicable to the Company, its vendors, partners, and any external parties involved in client referral, client onboarding and transaction processing.

[2] A relevant employee, is one whose work is: relevant to the firm's compliance with any requirement in the client operation; or otherwise capable of contributing to the: a) identification or mitigation of the risks of AML & CFT to which the firm's business is subject; or b) prevention or detection of AML & CFT risks in relation to the firm's business.

This section of the Policy provides an overview of the internal adopted measures, while the more detailed procedures are outlined in the AML Manual and shall be complied with by all relevant employees, alongside this Policy document.

Below is the summary of internal measures and controls, adopted by the Company and governing its day-to-day operations:

- the Company's governance structure allows for adequate segregation of functions between senior managers in charge of oversight and effective management of all matters related to financial crime risks, and is properly formalized in the Statement of Roles & Responsibilities document;
- the senior managers' roles and assigned responsibilities in relation to managing financial crime risks, developing and providing oversight over the firm's internal systems and controls are clearly defined in the Statement of Roles & Responsibilities approved by the Company's Board of Directors;
- the financial crime risks are identified and assessed as part of the Company's business-wide risk assessments and AML risk assessments, which are produced annually and, when necessary, or as required by the senior management. The priority is given to the risks that have a greater chance of materializing, and may cause a bigger impact for the Company, and, to adequate allocation of resources required to manage the risks effectively;
- the sufficient level of oversight on the part of the Board of Directors is established through regularly produced management information, that also ensures the effectiveness of the development and implementation of the measures and remediation plans, designed to tackle the financial crime risks identified during risk assessments.

The following management information is produced internally:

- Quarterly detailed financial crime reports (incl. AML reports);
- Money Laundering Risk Assessments produced at least annually;
- Annual report prepared by the MLRO and reviewed by the Board of Directors;

- Internal audit reports prepared annually or as often as required.

The Company does not underestimate the importance of the role that its employees play in tackling money laundering and other financial crime risks, as well as safeguarding the integrity, reputation and high-standards of conduct within the Company. The Company's vetting process and KYE policies, therefore, ensure the integrity and expertise of all relevant employees on an ongoing basis. All relevant employees, including MLRO and senior managers, undergo regular AML training and awareness sessions and are kept aware of their responsibilities and obligations in respect to AML and CFT, as well as recent legislative and regulatory developments in this area, and any changes in the Company's policies and procedures.

13. Client Onboarding and Acceptance

The following are the broad guidelines in respect to client onboarding:

a) all clients have to submit Proof of Identity that must be fully legible, colored with clear and identifiable photography and a signature which is the same signature in Client's application form.

- Client's valid passport,
- Identification Card,
- Driver's License.

For verification of the client, current permanent address must be verified via Proof of Residence (POR). POR must be issued in the individual's name and must contain the individual's residential address. Cannot be older than 3 months and cannot be the same as the document provided as proof of identity. Any of the following must be submitted:

- utility bill (electricity or water authority bill, internet or phone services bill)
- bank statement (current, deposit or credit card account)

The detailed procedure is stipulated in the Client Identification and Due Diligence section of the AML Manual.

b) all clients are screened against Risk Screening Tool database, in order to ensure that the identity of the client in question does not match with any persons who are known to have criminal background or are subject to sanctions, or is associated with banned entities such as individual terrorists or terrorist organizations, etc. In addition, the clients are screened against records of PEPs (including their close associates and family members), which are also covered in the Risk Screening Tool database;

c) all clients are classified into different risk categories in line with the provisions of the Client Classification section of the AML Manual. The following risk factors, inter alia, are accounted for when considering the level of risk involved with each client relationship: cumulative amount of funds deposited into the client account/accounts, country of residence, nationality, results of risk screening etc. Depending on the level of risk assigned to the client, additional checks may be required for those clients, falling within higher risk categories. Enhanced due diligence is conducted for such clients, whereby the source of funds and/or source of wealth, and any other information deemed necessary, are verified additionally to the checks conducted within the standard due diligence. The classification of clients, according to their risk profile, then serves the Company to set the appropriate rules for ongoing monitoring of the relationship and transactions. The detailed Client Due Diligence procedures are laid out in the relevant section of the AML Manual;

d) following the necessary checks, and, based on the perceived level of risk, associated with each client relationship, the decision is made to either proceed with a client's application or reject it. For all the clients classified as high-risk, an approval from either the MLRO, or the CEO is required;

e) PEPs, their family members and close associates are classified as higher-risk and must undergo enhanced due diligence procedure;

f) the Company's Client Acceptance Policy (CAP) lays down the criteria for accepting of the clients. The detailed provisions of CAP are specified in AML Manual. The following client

categories, inter alia, are not accepted by the Company as clients (the list below is not exhaustive):

- where sufficient KYC information could not be obtained/confirmed or as per the risk categorization;
- the client matches the person in the sanction lists during risk screening and the match is confirmed to be a true match by the designated compliance officer or the MLRO;
- the client matches the person in the lists with criminal records during World-Check screening and the match is confirmed to be a true match by the designated compliance officer or the MLRO;
- clients from countries on the list of non-cooperatives jurisdictions with FATF;
- clients from USA, Mauritius;
- client accounts are in names of companies, the shares of which are in bearer form;
- the client is a Trust account.

14. Ongoing Client Monitoring

The ongoing monitoring arrangements are comprised of two sets of measures:

(1) First, the client records are kept up-to date, KYC information and documents are updated regularly; these updates, for instance, include ongoing World-Check screening for all existing client base. The client information updates may result in re-classification of the client into a different risk category, in which case, the rules for ongoing monitoring over this client relationship are re-set to align with the updated risk category;

(2) In line with the risk classification of a client relationship, the transaction monitoring rules are designed for the specific client, and ongoing monitoring of that client's activity is conducted manually by the relevant employees, in "real-time" and retrospectively.

15. Internal and External Reporting

All employees must be aware of their obligation on reporting suspicious activity where they have knowledge or grounds for suspicion. For further guidance on what constitutes grounds for suspicion and what constitutes suspicious activity, please refer to the "Recognition and Reporting of Suspicious Activity" section of the AML Manual.

In case of suspicion, all employees must fill in the Internal Suspicious Activity Report and send it directly to the MLRO for further investigation. No transacting with the client who is the subject of suspicion is allowed without the guidance from the MLRO. No disclosure is allowed, apart from the MLRO and the line manager, to anyone within the Company or to the client, for prevention of tipping-off and committing an offence. The detailed procedure for submitting Internal Suspicious Activity Report is outlined in the AML Procedures Manual.

The MLRO is responsible for reviewing all internal reports submitted to him and making a judgement when the report to the FIU must be made.

If no report to FIU is made, the reason must be recorded by the MLRO. The MLRO or deputy MLRO will commit a criminal offence if they know or suspect, or have reasonable grounds to do so, through a disclosure being made to them, that another person is engaged in money laundering and/or terrorist financing, and they do not disclose this as soon as practicable to the FIU.

The MLRO shall ensure that Company's employees of the various departments (including outsourced employees) receive AML training aimed at latest developments in the prevention of Money Laundering and Terrorist Financing as well as KYC, KYE policies and filing iSAR (internal Suspicious Activity Report) to the MLRO. The training will be set up annualy and may be organized in different levels based on the risk assessment which employees are dealing with.

Requirements for STR (Suspicious Transactions Report):

- Single deposit and cumulative deposit which are not consistent with the client's economic profile.
- Origin and/or destination of funds are from the Country of High Risk.
- Pass-through / in-and-out-transactions.
- Trading activities are not consistent with client's previous trading experience.
- An abnormal number of people trading on a particular outcome/product.
- Abnormally large trades being placed on a particular outcome.
- The client exhibits a lack of concern regarding risks, commissions, or other trading risks.

16. Record Retention

All data obtained according to client identification and AML security measures must be documented.
Records must be kept for a minimum of 7 years, notwithstanding potentially longer retention periods under local civil or commercial law.

The retention of relevant records is done in line with the regulatory obligations in Mauritius, and in line with the Company's internal policy, outlined in the AML Manual.

The MLRO is in charge of keeping records of all referrals received and any action taken to ensure an audit trail is maintained. All information obtained for the purposes of money laundering checks and referrals must be kept up-to-date.

17. Appendix 1. Glossary

AML	Anti-Money Laundering
SCR	Mauritius rupee
CAP	Client Acceptance Policy
CEO	Chief Executive Officer
CFT	Combatting the Financing of Terrorism
FATF	Financial Action Task Force
FSA	Financial Service Authority Mauritius
FIU	Finance Intelligence Unit (of Mauritius)
IOSCO	International Organization of Securities Commissions
KYC	Know Your Client
KYE	Know Your Employee
MLRO	Money Laundering Reporting Officer
PEP	Politically Exposed Person
SYSC	FCA's Systems and Controls
UN	United Nations