WUNDERSYS CAPITAL (MAURITIUS) LIMITED

Investment Dealer (Full-Service Dealer excl. Underwriting) License

ANTI MONEY LAUNDERING & COMBATTING THE FINANCING OF TERRORISM MANUAL

OCTOBER 2024

PRIVATE & CONFIDENTIAL

TABLE OF CONTENTS

Date of issue/update	Created: October 2024	Version 1
Policy owner	Compliance Manager	
Approved by	Board of Directors	03 November 2025

1. LIST OF ACRONYMS

Acronyms	Full Terms
AML	Anti - Money Laundering
AML/CFT	Anti - Money Laundering and Combatting of Terrorism Financing
BoM	Bank of Mauritius
CDD	Customer Due Diligence
CFT	Combatting Financing of Terrorism
CO	Compliance Officer
DMLRO	Deputy Money Laundering Reporting Officer
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FIAMLA	The Financial Intelligence and Anti - Money Laundering Act
FIAML	The Financial Intelligence and Anti - Money Laundering Regulations 2018
FCCA	Financial Crimes Commission Act 2023
FCC	Financial Crimes Commission
FIU	Financial Intelligence Unit
FSC	Financial Services Commission
ICAC	Independent Commission Against Corruption
ML	Money Laundering
MLRO	Money Laundering Reporting Officer
TF	Terrorism Financing

2. PURPOSE OF THE MANUAL

Pursuant to the Mauritian legislative framework, financial service providers are required to maintain written comprehensive compliance programs. The purpose of this **ANTI MONEY LAUNDERING & COMBATTING THE FINANCING OF TERRORISM MANUAL** (the "**Manual**" or "**Handbook**") is to provide staff members of **WUNDERSYS CAPITAL (MAURITIUS) LIMITED** (the "**Company**") with an overview of their responsibilities with regards to the Anti-Money Laundering and Combatting the Financing of Terrorism ("**AML/CFT**").

The Company is committed to follow best practices and market standards in areas of accountability, transparency and business ethics in order to promote sustainability. Adherence to AML/CFT is crucial and must be seen as an integral part of what you do on a daily basis. Failing to abide with these can have severe consequence, be it for you, the Company and Mauritius.

This Manual should not be seen as a replacement to the Handbook, as amended from time to time, issued by the FSC, to combat the Anti-Money Laundering Combatting & the Financing of Terrorism or any of the prevailing legislation including the Financial Intelligence and Anti Money Laundering Act 2002, the Financial Intelligence and Anti Money Laundering Regulations 2018, The United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019, the Anti-Money Laundering and Combatting the Financing of Terrorism and Proliferation (Miscellaneous Provisions) Act 2019 and the Anti-Money Laundering and Combatting the Financing of Terrorism and Proliferation (Miscellaneous Provisions) Act 2020.

Staff should refer to the FSC Handbook and Legislations should they be in doubt and clarification should be sought from either the Compliance/MLRO or the DMLRO or the Directors of the Company.

This Manual will be reviewed at least once on an annual basis. The Board of Directors will approve all changes made to this Manual. In the event of any inconsistency between this manual and the applicable laws and regulations or rules, codes, guidelines or similar instrument issued by the FSC or any other regulatory authority, the laws, regulations, rules, codes, guidelines shall prevail over this manual.

3. DEFINITIONS

Applicant for business	A person who seeks to establish a business relationship, or carries out an occasional transaction with the Company;
Beneficial Owner/ Beneficiary	(a) The natural person: who ultimately owns or controls a customer/client; or on whose behalf a transaction is being conducted; and (b) includes natural persons who exercise ultimate control over a legal person or arrangement and such other persons as are specified in regulations 6 and 7 of the Financial Intelligence and Anti-Money Laundering Regulations 2018;
Board	The board of directors of the Company;
Certified copy	Any copy document that has been certified as a true copy by a Suitable Certifier;

Customer/Client	A natural or legal person or legal arrangement for whom a transaction or account is arranged, opened or undertaken and includes – (a) a signatory to a transaction or account any person to whom an account or rights or obligations under a transaction have been assigned or transferred; any person who is authorised to conduct a transaction or control an account any person who attempts to take any action referred to above (e) an applicant for business;
Commercially Exposed Person	A person in the business world who has access to and potential influence over large, commercial operations (e.g., CEO or Director of major businesses);
Compliance	Conformity with the provisions of AML-CFT legislation including the Laws, Rules and Regulations and Guidance Notes in effect in Mauritius and this Compliance Manual;
Compliance Officer or CO	The Compliance Officer of the Company;
Compliant Jurisdiction	Countries listed as AML/CFT compliant/no international sanctions;
Customer Due Diligence ("CDD")	The process of obtaining and verifying identification information, which may also be in reference to the evidence itself;
Enhanced CDD	Additional CDD in respect of High-Risk Clients as required by this Compliance Manual;
FATF	Financial Action Task Force;
FATF Recommendations	The FATF Recommendations issued in February 2012 and are available at the website address of the FATF, www.fatf-gafi.org;
FATF Standards	The FATF Standards issued in February 2012 are available at the website address www.fatf-gafi.org;
Financial Institution	Under the Financial Intelligence and Anti- Money Laundering Act 2002, "financial institution" means an institution, or a person, licensed or registered or required to be licensed or registered under - (a) section 14, 77, 77A or 79A of the Financial Services Act; (b) the Insurance Act; or (c) the Securities Act or (d) the Captive Insurance Act 2015;
FIU Guidance Note 3	Suspicious Transaction Report - Guidance Note 3 as issued by the FIU under Section 10(2)(c) of the Financial Intelligence and Anti Money Laundering Act 2002 and which is effective as from 21st January 2014;

Funds	(a) any assets, including, but not limited to, financial assets, economic resources and property of every kind, whether tangible, intangible, movable or immovable, however acquired; (b) legal documents or instruments in any form – including electronic or digital, evidencing title to, or interest in, such funds or other assets; and including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, or letters of credit; any interest, dividends or other income on or value accruing from or generated by such funds or other assets, virtual or digital currencies, including cryptocurrencies; any other assets which potentially may be used to obtain funds, goods or services.
High Net-worth individual	"HNWI", designated person whose investible wealth exceed a substantial amount (such amount shall be determined on a case-to case basis and approved by the Senior Management of the Company)
Jurisdiction	For this Manual, Mauritius;
Manual	This Operations and Compliance Manual, its schedules, addenda and appendices and any revisions or Guidance Notes thereto, as may be published by the Company from time to time;
Money Lender	A person, other than a bank or a non-bank deposit taking institution, whose business is that of money lending or who provides, advertises or holds himself out in any way as providing that business, whether or not he possesses or owns property or money derived from sources other than the lending of money, and whether or not he carries on the business as a principal or as an agent;
NCCT List	The list of countries and territories identified from time to time by the FATF as Non-Co-operating Countries and Territories regarding AMLCFT:

Politically Exposed Persons	means a foreign PEP, a domestic PEP and an international organisation PEP; and for the purposes of this definition — "Domestic PEP" means a natural person who is or has been entrusted domestically with prominent public functions in Mauritius and includes the Head of State and of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials and such other person or category of persons as may be specified by a supervisory authority or regulatory body after consultation with the National Committee; "foreign PEPs" means a natural person who is or has been entrusted with prominent public functions by a foreign country, including Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of stateowned corporations, important political party officials and such other person or category of persons as may be specified by a supervisory authority or regulatory body after consultation with the National Committee; "international organisation PEP" means a person who is or has been entrusted with a prominent function by an international organisation and includes members of senior management such as directors, deputy directors and members of the board or equivalent functions, or individuals who have been entrusted with equivalent functions, including directors, deputy directors and members of the board or equivalent functions and such other person or category of persons as may be specified by a supervisory authority or regulatory body after consultation with the National Committee;
Recognised Exchange	Any of the stock exchanges and markets that are listed in the relevant guidance or legislation of the Jurisdiction;
Regulated Person	In relation to the Jurisdiction, a person carrying on relevant regulated financial services business as defined in the laws, rule and regulations of the Jurisdiction;
Reporting Authority or FIU	The Mauritius Financial Intelligence Unit (FIU);
STR	A suspicious transaction report, as defined in the laws, rule and regulations of the Jurisdiction and under the FIAMLA and made to the Reporting Authority;
Suitable Certifier	(i) A lawyer, notary, actuary, commissioner of oath, a member of the judiciary or a senior civil servant, accountant or other person holding a recognized professional qualification, a director or secretary (or authorized signatories) of a regulated financial institution in Mauritius or in an Compliant Jurisdiction, (ii) who clearly adds to the copy (by means of a stamp or otherwise) his name, address, position, capacity or profession and contact details to aid tracing of the certifier if necessary and (iii) who the Company believes in good faith to be acceptable and appropriate to it for the purposes of certifying;

Suspicious Transactions	Transaction(s) which: (1) give rise to a reasonable suspicion that it may involve a) the laundering of money or the proceeds of any crime; or b) funds linked or related to, or to be used for, terrorist financing, proliferation financing or by proscribed organisations, whether or not the funds represent the proceeds of a crime; (2) are made in circumstances of unusual or unjustified complexity; (3) appear to have no economic justification or lawful objectives; (4) are made by or on behalf of a person whose identity has not been established to the satisfaction of the person(s) with whom the transactions are made; or (5) give rise to suspicion for any other reason;
Terrorism	Under the Prevention of Terrorism Act 2002, Acts of Terrorism are defined as acts which: - (a) may seriously damage a country or an international organisation; and (b) are intended or can reasonably be regarded as having been intended to - (i) seriously intimidate a population; (ii) unduly compel a Government or an international organisation to perform or abstain from performing any act; (iii) seriously destabilise or destroy the fundamental political, constitutional, economic or social structures of a country or an international organisation; or (iv) otherwise influence such government, or international organisation; and (c) involves or causes, as the case may be - (i) attack upon a person's life which may cause death; (ii) attack upon the physical integrity of a person; (iii) kidnapping of a person; (iv) extensive destruction to a Government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property, likely to endanger human life or result in major economic loss; (v) the seizure of an aircraft, a ship or other means of public or goods transport; (vi) the manufacture, possession, acquisition, transport, supply or use of weapons, explosives or of nuclear, biological or chemical weapons, as well as research into, and development of, biological and chemical weapons; (vii) the release of dangerous substance, or causing of fires, explosions or floods, the effect of which is to endanger human life; (viii) interference with or disruption of the supply of water, power or any other fundamental natural resource, the effect of which is to endanger life;
Terrorist Property	Under the Prevention of Terrorism Act 2002, "terrorist property" means property which - (a) has been, is being, or is likely to be used for any act of terrorism;(b) has been, is being, or is likely to be used by a prescribed organisation; (c) is the proceeds of an act of terrorism; or (d) is gathered for the pursuit of, or in connection with, an act of terrorism;

4. MANAGEMENT AND RESPONSIBILITIES

Board Responsibility for Compliance

The Board of the Company is responsible for managing the organisation effectively and is in the best position to understand and evaluate all potential risks to the financial institution, including those of ML and TF. The Board must therefore take ownership of, and responsibility for, the business risk assessments and ensure that they remain up to date and relevant.

On the basis of its business risk assessment, the Board shall establish a formal strategy to counter money laundering and financing of terrorism. The Board will document its systems and controls (including policies and procedures) and clearly apportion responsibilities for countering money laundering and financing of terrorism, and particularly, the responsibilities of the Compliance Officer (the "**CO**") and Money Laundering Reporting Officer (the "**MLRO**") and the Deputy Money Laundering Reporting Officer (the "**DMLRO**").

The Company shall establish and maintain an effective policy, for which responsibility shall be taken by the Board, and such policy shall include provision as to the extent and frequency of compliance reviews. The Board should take a risk-based approach when defining its compliance review policy and ensure that those areas deemed to pose the greatest risk to the firm are reviewed more frequently.

As part of its compliance arrangements, the Company is responsible for appointing a CO, who is responsible for the implementation and ongoing compliance of the Company with internal programmes, controls and procedures in accordance with the requirements of the FIAMLA and FIAML Regulations 2018.

In addition to appointing a CO, an independent external audit function (yearly review) to test the ML and TF policies, procedures and controls of the financial institution should be maintained.

The Board must ensure that the compliance review policy takes into account the size, nature and complexity of the business of the Company, including the risks identified in the business risk assessments. The policy must include a requirement for sample testing of the effectiveness and adequacy of the financial institution's policies, procedures and controls.

The Board must document its systems and controls (including policies and procedures) and clearly apportion responsibilities for ML and TF, and, in particular, responsibilities of the MLRO and the CO.

The Board shall also establish documented systems and controls which:

undertake risk assessments of its business and its customers;

- determine the true identity of customers and any beneficial owners and controllers;
- determine the nature of the business that the customer expects to conduct and the commercial rationale for the business relationship;

- require identification information to be accurate and relevant;
- require business relationships and transactions to be effectively monitored on an ongoing basis with particular attention to transactions which are complex, both large and unusual, or an unusual pattern of transactions which have no apparent economic or lawful purpose;
- compare expected activity of a customer against actual activity;
- apply increased vigilance to transactions and relationships posing higher risks of ML/TF;
- ensure adequate resources are given to the compliance officer to enable the standards within this Handbook to be adequately implemented and periodically monitored and tested;
- ensure procedures are established and maintained which allow the MLRO and the DMLRO to have access to all relevant information, which may be of assistance to them in considering suspicious transaction reports ('**STR'**);
- require a disclosure to the FIU when there is knowledge or suspicion or reasonable grounds for knowing or suspecting ML and /or TF including attempted ML and/or TF; and
- maintain records for the prescribed periods of time.

5. MONEY LAUNDERING

Money laundering is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities. If undertaken successfully, it allows them to maintain control over those proceeds and, ultimately provides them with a legitimate cover for the source of their income.

It is vital in the fight against crime that criminals be prevented, whenever possible, from legitimizing the proceeds of their criminal activities by converting funds from 'dirty' to 'clean'.

Reference is made to s.36(1) of the FCCA

s36(1) Any person who —

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

(b) *receives, is in possession of, conceals, disguises, transfers, converts, disposes of, removes from or brings into Mauritius any property which is, or in whole or in part directly or indirectly represents, the proceeds of any crime, where he suspects or has reasonable grounds for suspecting that the property is derived or realized, in whole or in part, directly or indirectly from any crime, shall commit an offence.*

The laundering process is generally accomplished in three stages, as follows, which may comprise numerous transactions by the launderers that could trigger suspicion on money laundering.

1) **Placement** -the physical disposal of the initial proceeds derived from illegal activity.

2) **Layering** - separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity.

3) **Integration** -the provision of apparent legitimacy to criminally derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as normal business funds.

The three basic steps may occur as separate and distinct phases. They may also occur simultaneously or, more commonly, they may overlap. How the basic steps are used depends on the available laundering mechanisms and the requirements of the criminals.

6. Terrorist Financing

Terrorism Financing is the financial support, in any form, of terrorism or those who encourage, plan or engage in terrorism. A terrorist financier may only need to disguise the origin of the property if it was generated from criminal activity but in vast majority cases, they will seek to disguise the intended use.

The traditional terrorism financing model involves a series of transactions, generally considered as complex series of transactions, generally considered as representing three separate phases, namely:

1. **Collection** - Funds are often acquired through seeking donations, carrying out criminal acts or diverting funds from genuine charities.
2. **Transmission** - Where funds are pooled and transferred to a terrorist or terrorist group
3. **Use** - Where the funds are used to finance terrorist acts, training, propaganda etc.

The Company has to take reasonable steps through the internal controls to ensure that its services are not being used for criminal activities linked to terrorist financing.

7. Obligations of Financial Institutions

In order to combat money laundering and the financing of terrorism, every financial institution must take measures to ensure that neither it nor any services offered by it is capable of being used to commit or facilitate the commission of a money laundering and/ or terrorist financing offence.

Reference is made to s.36(2) of the FCCA:

S36(2) of the FCCA dictates that a reporting person who fails to take such measures as are reasonably necessary to ensure that neither he, nor any service offered by him, is capable of being used by a person to commit or to facilitate the commission of a money laundering offence or the financing of terrorism shall commit an offence and shall, on conviction, be liable to a fine not exceeding 20 million rupees and to penal servitude for a term not exceeding 10 years.

In addition, financial institutions have, in terms of the FIAMLA, a duty to verify the true identity of the clients and other persons with whom they conduct transactions.

8. PROLIFERATION FINANCING

Legal Framework

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 on the 21 May 2019 and both acts came into operation on the 29 May 2019.

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

What is Proliferation?

Proliferation refers to the development and use of nuclear, chemical, or biological weapons and their delivery systems — also referred to as weapons of mass destruction ("**WMD**") — by state or non-state actors in violation of international agreements and export control regimes.

In Mauritius, "proliferation" is defined under s.2 of the FIAMLA and means -

(a) *the manufacture, production, possession, acquisition, stockpiling, storage, development, transportation, sale, supply. transfer, import, export, transhipment or use of—*

(i) nuclear weapons
(ii) chemical weapons
(iii) biological weapons
(iv) such materials, as may be prescribed, which are related to nuclear weapons, chemical weapons, or biological weapons; or

(b) *the provision of technical training, advice, service, brokering, or assistance related to any of the activities specified in paragraph (a).*

What is the Financing of Proliferation of Weapons of Mass Destruction?

Proliferation of WMDs can be in many forms, but ultimately involves the transfer or export of technology, goods, software, services or expertise that can be used in programmes involving nuclear, biological or chemical weapons, and their delivery systems (such as long-range missiles).

Proliferation of WMD financing is an important element and, as with international criminal networks, proliferation support networks may use the international financial system to carry out transactions and business deals. Unscrupulous persons may also take advantage of the potential profits to be made by facilitating the movements of sensitive materials, goods, technology, and expertise, providing seemingly legitimate front organisations, or acting as representatives or middlemen.

All staff of the company should be adequately trained in ML, TF and PF including the CO, MLRO and DMLRO. The frequency of the training can be assessed based on the complexity of the nature of the business but should be at least once a year.

9. Targeted Financial Sanctions

What are sanctions?

A sanction is a measure adopted, usually by several nations acting together, against an entity, individual, country, regime or organisation believed to be violating international law. Measures may be economic, diplomatic, cultural, to deter, prevent and suppress the financing of terrorism or of some other type. They may include the freezing of financial assets, a ban on the trade of goods or weapons, and travel restrictions on individuals.

Some sanction orders will give a specific period of duration (in which case they will need to be extended or renewed if they are to continue). Others will not have a time limit and will need to be revoked if they are no longer to apply.

The UNSC has imposed sanctions to prevent and counter the proliferation of WMD, and its financing. This includes targeted financial sanctions against specific persons and entities that have been identified as being connected to the proliferation of Weapons of mass destruction ("WMD"). All UN member states are required to implement these measures.

Obligations

The UNSC has imposed sanctions to prevent and counter the proliferation of WMD, and its financing. This includes targeted financial sanctions against specific persons and

entities that have been identified as being connected to the proliferation of WMD. All UN member states are required to implement these measures.

Recommendation 7 of the FATF Standards requires countries to implement proliferation-related targeted financial sanctions (TFS) made under UNSC Resolutions without delay.

FATF Recommendation 7

"Countries should implement targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. These resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the United Nations Security Council under Chapter Vll of the Charter of the United Nations. "

Reporting Obligations & Procedures

Sanctions Reports -

If a true match is identified by a reporting person, it must immediately submit a report to the National Sanctions Secretariat, and in some cases also to its relevant supervisory authority.

Reports may be completed using the template which can be downloaded from the NSSec website:

Reports must be submitted to the following email address: nssec@govmu.org.

Understanding Sanctions Evasion

Common sanctions evasion techniques used by proliferators include:

a. The use of aliases and falsified documentation to hide involvement of listed party.
b. Bank accounts owned by nationals not from a proliferating country, who act as financial representatives on behalf of listed parties from the proliferating country.
c. Offshore, front and shell companies to hide beneficial ownership information, and the involvement of listed parties.
d. Listed parties entering joint ventures with non-listed companies.
e. Use of diplomatic staff bank accounts, on behalf of listed parties and proliferating countries.
f. Use of virtual currencies by listed parties to circumvent the formal financial system and evade sanctions.

g. Conduct cyber-attacks against financial institutions and crypto currency exchanges to raise funds and evade sanctions.

The United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 is the Company's primary sources of law in matters of Targeted Financial Sanctions.

10. Obligations under FIAMLA

The company's obligations under the above legislations include:

1. Maintaining a record of prescribed transactions
2. Furnishing information of prescribed transactions to the specified authority
3. Verifying and maintaining records of the identity of its clients
4. Keeping records in respect of (1), (2) and (3) above for a period of seven years from the date of cessation of transactions with the customers
5. In addition, the company will take such measures as are reasonably necessary (through an effective internal control) to ensure that it will not be used by any person to commit or to facilitate the commission of money laundering and / or terrorist financing.

11. Financial Crimes Commission Act 2023

The Financial Crimes Commission ("**FCC**") Act effective as from (29 March 2024) establishes a new independent body corporate to combat financial crimes both domestically and internationally for cases linked to Mauritius. The Prevention of Corruption Act, the Asset Recovery Act and the Good Governance and Integrity Reporting Act have been repealed and replaced by this new overarching legal framework. This implies that the FCC has taken over the functions of the Independent Commission Against Corruption, the Asset Recovery Investigation Division and the Integrity Reporting Services Agency. The FCC is also the depository for declarations made under the Declaration of Assets Act.

The FCC is responsible for:

1. receiving and considering allegations or complaints of financial crimes and referring these for investigations;
2. detecting and investigating into financial crimes and other offences through various specialised divisions;
3. educating the public to prevent financial crimes and any other offence under the FCC Act and the Declaration of Assets Act through its Education and Prevention Division;
4. prosecuting financial crimes and any other offence under the FCC Act and the Declaration of Assets Act; and
5. taking any other actions necessary to address financial crimes and other offences under the FCC Act and the Declaration of Assets Act.

The FCC Act describes in detail the different acts that would constitute corruption, money laundering offences, fraud, financing drug dealing offences and specifies the penalties applied in each case. This information is summarised in the table 1 below:

Offence	**Penalty**
Corruption	
Bribery by public official	Fine not exceeding 20 million rupees and to penal servitude for a term not exceeding 10 years
Bribery of public official	
Taking gratification to screen offender from punishment	
Public official using his office for gratification	
Bribery of, or by, public official to influence the decision of public body	
Influencing public official	
Traffic d'influence	
Public official taking gratification	
Bribery for procuring contracts	
Bribery for procuring withdrawal of tenders	
Conflict of interests	
Treating of public official	
Receiving gift for corrupt purpose	
Corruption in private entities	
Corruption to provoke serious offence	
Bribery by, or of, foreign public official	
Corruption in relation to sporting events	
Money Laundering	
Money laundering	Fine not exceeding 20 million rupees and to penal servitude for a term not exceeding 10 years
Limitations of payment in cash	
Fraud	
Fraud by false representation	
Fraud by failing to disclose information	

Making or supplying articles for use in fraud offence	Fine not exceeding 20 million rupees and to penal servitude for a term not exceeding 10 years
Failing to pay for goods and services	
Fraud by abuse of position	
Electronic fraud	
Financing Drug Dealing	
Financing of drug dealing	Fine not exceeding 20 million rupees and to penal servitude for a term not exceeding 10 years
Other Offences	
Making or supplying articles for use in the course of or in connection with an offence	Fine not exceeding 5 million rupees and to imprisonment for a term not exceeding 5 years
Possession of articles use in the course of or in connection with an offence	Fine not exceeding 5 million rupees and to imprisonment for a term not exceeding 5 years
Conspiracy	Fine not exceeding 20 million rupees and to penal servitude for a term not exceeding 10 years
Aiding, abetting or counselling	Fine not exceeding 20 million rupees and to penal servitude for a term not exceeding 10 years
Attempt to commit an offence	Fine not exceeding 5 million rupees and to imprisonment for a term not exceeding 5 years
Penalty for breach of guidelines	Penalty representing 10,000 rupees per month or part of the month, until such time as the breach is remedied, provided that the total penalty payable shall not exceed one million rupees
Obligations and Liability of Legal Persons	
Obligations of legal persons	Fine not exceeding 20 million rupees
Liability of legal persons	

12. Why AML/ CFT Policy?

a. To prevent criminal elements from using the Company for money laundering and / or terrorist financing activities.
b. To enable the Company to know / understand the clients and their financial dealings better, which in turn would help to manage risks prudently.
c. To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws and laid down procedures.
d. To comply with applicable laws and regulatory guidelines.
e. To take necessary steps to ensure that the relevant staff are adequately trained in KYC/AML procedures.

13. REPORTING OBLIGATIONS & PROCEDURES

Every financial institution has a duty under the FIAMLA to forthwith make a report to the FIU of any transaction which the financial institution has reason to believe may be a suspicious transaction. Financial institutions are required to use the goAML platform of the FIU to report suspicious transactions. The contact details of the FIU are as follows:

The Director
Financial Intelligence Unit
7th Floor, Ebéne Heights
34, Ebéne Cybercity
Ebéne

Republic of Mauritius
Tel: (230) 4541423
Fax: (230) 466 2431
Email: fiu@tiumauritius.org

14. SUSPICIOUS TRANSACTIONS

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

Suspicious transactions provide reasonable grounds to suspect that such transactions are related to the commission of a money laundering (ML) or terrorism financing (TF) offence.

The FIU, as the central agency in Mauritius responsible for receiving, requesting, analysing and disseminating disclosures of information, is determined on fostering a vibrant STR reporting culture. The Company has certain obligations set out under the Financial Intelligence and Anti Money Laundering Act (FIAMLA) and one of the obligations relates to the filing of STRs to the FIU.

As soon as the Reporting Persons become aware of a suspicious transaction, they are required to make a report to FIU of such transaction not later than 5 working days after the suspicion arose. Failure to report STRs is a criminal offence and on conviction and liable to a fine not exceeding 5 million rupees and to imprisonment for a term not exceeding 10 years.

STRs are highly confidential and should not be disclosed to any other person than the FIU. Any such disclosure would amount to tipping off, which is a criminal offence pursuant to section 16(1) of FIAMLA. The FIU, as bound by FIAMLA, does not disclose the source of any STR filed and the source remains strictly confidential.

How to identify a suspicious transaction?

There is no monetary threshold for making a report concerning a suspicious transaction. A suspicious transaction may involve several factors that may on their own seem insignificant, but when taken together, may raise suspicion that the transaction is related to the commission or attempted commission of a money laundering offence.

As a general guide, a transaction may be connected to a money laundering offence when one thinks that it (or a group of transactions) raises questions or gives rise to discomfort, apprehension or mistrust.

The context, in which the transaction occurs or is attempted, is a significant factor in assessing suspicion. This will vary from business to business and from one Client to another. The Company should evaluate transactions in terms of what seems appropriate and is within normal practice in its particular line of business, and based on its knowledge of the Client. The fact that transactions do not appear to be in keeping

with normal industry practices may be a relevant factor for determining whether there are reasonable grounds to suspect that the transactions are related to money laundering.

An assessment of a suspicion should be based on a reasonable evaluation of relevant factors, including the knowledge of the Client's business, financial history, background and behaviour. It is important to remember that it is the behaviour, which is suspicious, not the person. Also, it could be the consideration of many factors, not just one factor, which will lead to a conclusion that there are reasonable grounds to suspect that a transaction is related to the commission or attempted commission of a money laundering offence. All circumstances surrounding a transaction(s) should be reviewed.

Indicators of suspicious transactions

The indicators that follow are provided to help assess whether or not transactions might give rise to reasonable grounds for suspicion. They are examples of common and industry-specific indicators that may be helpful when evaluating transactions, whether completed or proposed. These indicators include indicators, which is based on certain characteristics that have been linked to money laundering in the past.

The indicators emanate from money laundering typologies and/or trends as experienced and developed in other jurisdictions. As money laundering is a global phenomenon, these typologies and/or trends are relevant and helpful to reporting entities in that they reflect a pattern or behaviour that prompts deployment of diligence in any given transaction. These indicators are not intended to cover every possible situation and are not to be viewed in isolation. As such, a single indicator is not necessarily indicative of reasonable grounds to suspect money laundering. However, if a number of indicators are present during a transaction or a series of transactions, then the Company might want to take a closer look at other factors prior to making the determination as to whether the transaction must be reported.

The indicators have to be assessed in the context in which the transaction occurs or is attempted. Each indicator may contribute to a conclusion that there are reasonable grounds to suspect that the transaction is related to the commission or attempted commission of a money laundering offence. However, it may also offer no indication of this in light of factors such as the Client's occupation, business, financial history and past investment pattern. Taken together, the presence of one or more indicators as well as the Company's knowledge of its Client's business or financial affairs may help the Company in identifying suspicious transactions.

Becoming aware of certain indicators could trigger reasonable grounds to suspect that one or more transactions from the past (that had not previously seemed suspicious) were related to money laundering. For example, this could happen if it were reported in the media or some other reliable source that one of the Company's Clients is suspected of being involved in illegal activity. If this amounts to suspicion regarding a

previous transaction with this Client, the Company would have to report it to the FIU as soon as practicable but not later than five (5) days after establishing a suspicion.

15. MONITORING OF TRANSACTIONS

The Company has systems in place to detect complex, unusual or suspicious transactions or patterns of activity for all accounts. It has also established and maintain adequate systems and processes to monitor transactions. The design, degree of automation and sophistication of transaction monitoring systems and processes have been developed appropriately having regard to the following factors:

a. the size and complexity of its business;
b. the ML/TF risks arising from its business;
c. the nature of its systems and controls;
d. the monitoring procedures that already exist to satisfy other business needs;
e. the nature of services provided;
f. the transaction is international in nature, does the clients have any obvious reason for conducting business with the other country involved;
g. significant transactions (in terms of amount or volume) for that client;
h. the transactions that exceed transaction or amount limits;
i. the geographical origin/destination of a transaction (jurisdictions that pose a higher risk to their particular sector or client type;
j. transactions made by clients which pose higher money laundering and terrorism financing risks, such as High Net Worth Individuals, Politically Exposed Persons amongst others;
k. the transactions outside the regular pattern of an account's activity; and
l. unusual flow of funds.

16. WHY DO WE HAVE SUSPICIOUS TRANSACTION PROCEDURES?

Not all unusual or suspicious transactions will be cases of money laundering or funds gained from illicit activity. However, there is a duty to report cases that are found to be "suspicious" and let the proper investigations be conducted.

It is extremely important for staff to understand what they are doing and to not merely do as they are told. Members of staff are requested to use a logical and common-sensical approach and always attempt to decipher the reason for a particular transaction or state of affairs. If something does not make sense or cannot be explained according to the surrounding circumstances of a particular business or transaction, then staff should forthwith notify the MLRO.

It is the duty of the employee under the law to make a report of any suspicious transaction that he/she comes across and where an employee makes a STR to the

MLRO, he/she will have discharged his/her legal obligation to report under the FIAMLA 2002.

The STR should be remitted directly to the MLRO or the Deputy MLRO and not be compromised by any other staff within the Company.

All KYC details need to be rigorously screened and investigated by the MLRO and any other employee that might be more familiar with the client details to determine whether the STR has any foundation. All contributions and memos should be made in writing.

If the investigation can unequivocally be found to be without foundation, then the matter is closed, and the findings logged.

If there is any remaining suspicion, no matter how trivial, then a full external report must be submitted to the FIU through the goAML platform, and the relevant details entered into the STR log.

17. DUTIES UNDER FIAMLA AND FIAML REGULATIONS 2018

Section 14(1) of the FIAMLA states that:

"[...]every reporting person or auditor shall, as soon as he becomes aware of a suspicious transaction, make a report to FIU of such transaction not later than 5 working days after the suspicion arose."

Section 17(1) of the FIAMLA states that:

(1) "Every reporting person shall —

a. *take appropriate steps to identify, assess and understand the money laundering and terrorism financing risks for customers, countries or geographic areas and products, services, transactions or delivery channels; and*

b. *consider all relevant risk factors before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied".*

(3) *"Prior to the launch of a new product or business practice or the use of a new or developing technology, a reporting person or a supervisory authority shall identify and assess the money laundering or terrorism financing risks that may arise in relation to such new products or business practices, or new or developing technologies for both new and pre-existing products and take appropriate measures to manage and mitigate these risks."*

(4) *"Every reporting person shall document the risk assessments in writing, keep it up to date and, on request, make it available to relevant competent authorities without delay."*

Regulation 22 of the FIAML Regulations 2018 states that:

"22. (1) Every reporting person shall implement programmes against money laundering and terrorism financing having regard to the money laundering and terrorism financing risks identified and the size of its business, which at a minimum shall include the following internal polices, procedures, and controls —

(a) designation of a compliance officer at senior management level to be responsible for the implementation and ongoing compliance of the reporting person with internal programmes, controls and procedures with the requirements of the Act and these regulations; (b) screening procedures to ensure high standards when hiring employees;

(C) an ongoing training programme for its directors, officers, and employees to maintain awareness of the laws and regulations relating to money laundering and terrorism financing to —

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

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

(d) an independent audit function to review and verify compliance with and effectiveness of the measures taken in accordance with the Act and these regulations.

This Regulation should be read in conjunction with Chapter 12 of the FSC Handbook 2020.

18. IDENTIFYING A SUSPICIOUS TRANSACTION

Refer to the Guidance Note 4 issued by the Financial Intelligence Unit (FIU), in force with effect in November 2020 for information inter alia on how to identify a Suspicious Transaction.

This Guidance Note has been prepared pursuant to section 10(2)(c) of the FIAMLA and is intended, inter alia, to guide Money Laundering Reporting Officers (and their Deputies) in completing the Suspicious Transaction Report form issued by the FIU. It is provided as general information only and it is not intended to act as a substitute for your own assessment, based on your own judgement, knowledge as well as on the specific circumstances of the transaction.

19. INTERNAL PROCEDURE FOR THE REPORTING OF SUSPICIOUS TRANSACTIONS

Staff must report any suspicious transaction to the MLRO" using the Internal Disclosure Form, in order to discharge their reporting legal obligations.

The MLRO will review the matter and evaluate the Internal STR Report, after which a report to the FIU will be made as and when required.

In the absence of the MLRO, any suspicious transaction should be reported to the Deputy MLRO on the Internal STR Form.

The Compliance Officer will maintain an Internal STR Register, in which all the internal suspicious transactions which have been reported to the MLRO/Deputy MLRO will be recorded as well as an external STR Register whereby all the external suspicious transactions reported to the FIU will be recorded.

20. DUE DILIGENCE

The key to the prevention and detection of money laundering and the financing of terrorism lies in the implementation of; and strict adherence to, effective systems and controls, including sound customer due diligence (the "**CDD**") measures based on international standards.

The FIAMLA and the Reg 2018 provides that the Entity as a reporting person must undertake CDD measures when establishing a business relationship or for a one-off transaction.

The Company must undertake CDD measures and be satisfied of the results obtained:

a. In cases of one-off transactions or a series of occasional transactions where the total amount of the transactions which is payable by or to the applicant for business is above 500,000 Mauritian Rupees or an equivalent amount in foreign currency; or

Whenever there is a suspicion of money laundering or terrorist finding at any point in time since the inception till the termination of the business relationship.

In line with the Handbook, the Entity is required to collect information on any prospective client, carry out an assessment and evaluation and determine the initial risk rating. Based on the initial risk rating, additional information and documentation might be collected. Further assessment and evaluation will be carried out to confirm the risk rating and conduct on-going due diligence according to the risk rating obtained.

The Handbook is intended for use by financial service businesses to develop systems and controls and details policies and procedures to ensure compliance with The FIAMLA and the Reg 2018. These policies and procedures have been written using the Handbook as reference.

To assist the overall objective to prevent money laundering and the financing of terrorism, these procedures adopt a risk-based approach. They recognise that the money laundering and financing of terrorism threat to the Company varies across clients, countries and territories, products and delivery channels.

The procedures allow the Company's personnel to identify and manage the various risks in a way that matches the Company's risk appetite while establishing minimum standards that will allow the Entity to apply its own approach to systems and controls, and arrangements in particular circumstances. Effective CDD is vital to facilitate activity monitoring procedures.

Failure to follow the Company's procedures to ensure satisfactory CDD measures are undertaken and maintained, exposes both the Company, its directors and its officers to Client and counterparty risks as well as reputational.

No business (which for the avoidance of doubt includes the receipt of funds or assets of any kind) is to be conducted with any individual or entity, until such time as identity has been satisfactorily verified.

The Politically Exposed Persons ("**PEP**") procedure detailed in the Internal Procedures and Control Manual must be followed with respect to the acceptance of all new PEP relationships.

21. TIPPING OFF

S. 19(1)(c) of the FIAMLA provides for the offence of tipping off - which offence is committed when a person, knowingly or without reasonable excuse, warns or informs the owner of any funds of any report or any action that is to be taken in respect of any transaction concerning such funds.

The FIAMLA expressly prohibits a person who is directly or indirectly involved in the reporting of a suspicious transaction from divulging to any person involved in the transaction or to any unauthorized third party with the exception of the Regulatory Body that the transaction has been reported.

In practice, preliminary enquiries in respect of an applicant for business, either to obtain additional information to confirm true identity, or to ascertain the source of funds or the precise nature of the transaction being undertaken, will not trigger a 'tipping off offence. Great care should, however, be taken where a suspicious transaction has already been reported and it becomes necessary to make further enquiries, to ensure that customers do not become aware that their names have been brought to the attention of the FIU.

22. FAILURE TO REPORT

Any financial institution or any director or employee thereof who knowingly or without reasonable excuse fails to lodge a report of a suspicious transaction, commits 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.

23. SANCTIONS

Where it appears to the Regulatory Body that any financial institution subject to its supervision has failed to comply with any requirement imposed by FIAMLA or any regulations applicable to that financial institution and that the failure is caused by a negligent act or omission or by a serious defect in the implementation of any such requirement, the FSC, in the absence of any reasonable excuse, may sanction the company / individual as per the applicable laws.

24. TRAINING

Obligations -

The Company is required, under Regulation 22(1)(c) of FIAML Regulations to carry ongoing training programmes for directors, officers and employees in order for them to maintain awareness of the laws and regulations relating to money laundering and terrorism financing and to (i) assist them in recognising transactions and actions that may be linked to money laundering or terrorism financing; and (ii) instruct them in the procedures to be followed where any links have been identified under sub subparagraph (i).

Training Requirements -

As per Chapter 12 of the FSC Handbook, all employees are made aware of the Company's Internal Control, Policies and Procedures. They are also informed of the identity of the MLRO and the Deputy MLRO as well as their responsibilities.

The Company would ensure that all its employees are appropriately trained and that the training programmes are designed in such a way that the following important aspects are covered:

- Legal obligations as well as aspects of the AML/CFT laws, regulations and guidelines;
- The money laundering and terrorism financing vulnerabilities of the products and services offered by the Company;
- The CDD requirements and the requirements for the internal and external reporting of suspicion;
- Recognition and handling of suspicious transactions/activities;
- The criminal sanctions in place for failing to report information;
- New developments including information on current money laundering and terrorist financing techniques, methods, trends and typologies; and

- Information on the changing behaviour and practices amongst money launderers and those financing terrorisms.

Employees would be provided with a minimum of at least one training session annually.

A copy of training records will have to be shared with the CO.

In accordance with Regulation 22(1)(c) of FIAML Regulations 2018, the ongoing training provided by the company shall cover:

1. the FIAMLA, FIAML Regulations 2018, any AML/CFT Code issued by the FSC and its guidance;
2. the implications of non-compliance by employees to requirements of FIAMLA, FIAML Regulations 2018, any AML/CFT Code issued by the FSC and guidance; and
3. the company's policies, procedures and controls for the purposes of foreseeing, preventing and detecting ML and TF.
4. Wundersys Capital (Mauritius) Limited shall, in addition shall ensure that the ongoing training provided to directors, officers and employees also covers, to a minimum:

    a. the requirements for the internal and external disclosing of suspicion;
    b. the criminal and regulatory sanctions in place, both in respect of the liability of the company and personal liability for individuals, for failing to report information in accordance with the policies, procedures and controls of the company;
    c. the identity and responsibilities of the MLRO, CO and Deputy MLRO;
    d. dealing with business relationships or occasional transactions subject to an internal disclosure, including managing the risk of tipping off and handling questions from customers;
    e. those aspects of the company's business deemed to pose the greatest ML and TF risks, together with the principal vulnerabilities of the products and services offered by the company, including any new products, services or delivery channels and any technological developments;
    f. new developments in ML and TF, including information on current techniques, methods, trends and typologies;
    g. company's policies, procedures and controls surrounding risk and risk awareness, particularly in relation to the application of CDD measures and the management of high risk and existing business relationships;
    h. the identification and examination of unusual transactions or activity outside of that expected for a customer;
    i. the nature of terrorism funding and terrorist activity in order that employees are alert to transactions or activity that might be terrorist-related;
    j. the vulnerabilities of the company to financial misuse by PEPs, including the effective identification of PEPs and the understanding, assessing and handling of the potential risks associated with PEPs; and
    k. UN, EU and other sanctions and the company's controls to identify and handle natural persons, legal persons and other entities subject to sanction.

Additional Training requirement

1. The company shall also identify employees who, in view of their particular responsibilities, should receive additional and ongoing training, appropriate to their roles, and it shall provide such additional training.

2. This section set out those categories of employee who are to be provided with additional training, together with the particular focus of the additional training provided. The categories below are not exhaustive and the company may identify other employees who it considers require additional training.

3. The Board and Senior Management

(a) The Board and senior management shall receive adequate training to ensure they have the knowledge to assess the adequacy and effectiveness of policies, procedures and controls to counter the risk of ML and TF.

(b) The additional training provided to the Board and senior management must include, at least, a clear explanation and understanding of:

(i) offences and penalties arising for non-reporting or for assisting money launderers or those involved in terrorist financing;

(ii) requirements for CDD including verification of identity and retention of records; and

(iii) in particular, the application of the company's risk-based strategy and procedures.

4. The Money Laundering Reporting Officer and Deputy Money Laundering Reporting Officer

(a) Ongoing professional development, including participating in professional associations and conferences, is vital for MLROs/ DMLROs. In addition, MLROs and DMLRO should receive in depth training on all aspects of the prevention and detection of ML/TF, including, but not limited to:

(i) AML/CFT legislative and regulatory requirements;

(ii) the international standards and requirements on which the Mauritius' strategy is based, namely the FATF 40 Recommendations and ML/TF typology reports that are relevant to their business;

(iii) the identification and management of ML/TF risk;

(iv) the design and implementation of internal systems of AML/CFT control;

(v) the design and implementation of AML/CFT compliance testing and monitoring programs;

(vi) the identification and handling of suspicious activity and arrangements and suspicious attempted activity and arrangements;

(vii) the money laundering and terrorist financing vulnerabilities of relevant services and products;

(viii) the handling and validation of internal disclosures;

(ix) the process of submitting an external disclosure;

(x) liaising with law enforcement agencies;

(xi) money laundering and terrorist financing trends and typologies; and

(xii) managing the risk of tipping off.

5. The Compliance Officer

(a) The CO is responsible for ensuring continued compliance with the requirements of FIAMLA and FIAML Regulations 2018 and having an overall oversight of the program for combatting money laundering and terrorism financing amongst others (Regulation 22(3) of FIAML Regulations 2018).

(b) The CO should receive in depth training on all aspects of the prevention and detection of ML/TF, including, but not limited to, addressing the monitoring and testing of compliance systems and controls (including details of the company's policies and procedures) in place to prevent and detect ML and TF.

(c) Each employee is required to read and comply with this Compliance Manual, address any questions and concerns to the Director/Designated Staff.

(d) The training program will be conducted on an on-going basis. The frequency of the trainings will be determined on a risk-based approach, with those employees ("relevant employees") with the responsibility for handling of business relationships or business transactions receiving more frequent training but, in any case, at least once every year.

25. EMPLOYEE VETTING

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

a. obtaining and confirming details of employment history, qualifications and professional memberships;
b. obtaining and confirming appropriate references;
c. obtaining and confirming details of any regulatory action or action by a professional body taken against the prospective employee;
d. obtaining and confirming details of any criminal convictions, including the provision of a check of the prospective employee's criminal record; and
e. screening the employees against the UN's list of designated persons under terrorist and proliferation financing targeted financial sanctions

The Company shall:

a. assess the competence and probity of its Employees at the time of recruitment and at the time of any subsequent change to the Employee's role; and

b. monitor, on an ongoing basis, the competence and probity of its Employee's;

c. Where an employee is dismissed on account of short comings in relation to his/her competence with any anti-money laundering or terrorist financing requirements or his/her probity, the Company must within seven days of such dismissal provide written notification to the Authorities of the fact together with such information so as to enable the Authorities to understand the circumstances and reasons for the dismissal.

26. INDEPENDENT COMPLIANCE AUDIT POLICY

INTRODUCTION

The Independent AML/CFT Audit is as per the Chapter 13 of the FSC Handbook, and as required under Regulation 22(1)(d) of the FIAML Regulations 2018. This Policy defines the principles and commitments of the company regarding regulatory Compliance.

SCOPE OF INDEPENDENT AUDIT

The Independent Compliance Audit shall help to ascertain if the AML/CFT programme adopted by the Company throughout the specified period was adequate and effective

and advises on any changes that may be required. This shall be done by testing compliance in the following non-exhaustive areas:

a. AML/CFT Policies and Procedures
b. Internal Risk Assessments
c. Risk Assessments on the use of third-party service providers (Outsourcing)
d. Compliance Officer functions and effectiveness
e. MLRO/ Deputy MLRO functions and effectiveness
f. Implementation and Effectiveness of Mitigating Controls, including Customer Due Diligence and enhanced measures
g. AML/CFT Trainings
h. Record Keeping Obligations
i. Targeted Financial Sanctions
j. Suspicious Transaction Monitoring and Reporting

AUDIT FREQUENCY

The Independent Compliance Audit shall be conducted on an annual basis and/or when there has been a major change in the AML/CFT risk assessment, policies, or procedures. However, the audit frequency shall be based on the internal risk assessment and any previous audits.

INDEPENDENCE OF THE AUDITOR

The Independent Compliance Audit shall be independent and separate from the operational and executive team dealing with the AML/CFT processes. An independent audit review will be conducted by an internal or external audit professional. Apart from being independent, the choice of the auditor should be based on the experience and skill of the latter. The background and qualifications of the auditor shall be asked prior to the audit. In order to ensure that the audit is properly conducted as required under the FIAMLA and FIAML Regulations 2018, the audit professional needs to provide quality recommendations, so that can use the findings and recommendations to improve its internal process.

AUDIT REPORTING

Audit must be signed and cover results of reviews on above mentioned areas and shall be reported to senior management and the company's Board of Directors.

27. FILING TO THE FSC

The Company shall file its independent audit report for a specified period, upon the request of the FSC.

INDEPENDENT COMPLIANCE AUDIT POLICY REVIEW

This policy will be reviewed at a minimum annually or in the event of any changes in the law and/or any changes in our business practice.