COMPLIANCE & ANTI-MONEY LAUNDERING OPERATIONAL MANUAL

Mevora Capital

(THE "ENTITY")

Version	Date	Description
1.0	_____	AML Framework formulated by the Compliance Officer
1.0	_____	AML Framework ratified by the Board
V1.0	_____	Initial Issue

Table of Contents

This document provides an overview of the compliance framework for Mevora Capital, specifically regarding Anti-Money Laundering (AML) and Counter-Terrorism Financing (CFT) in accordance with the laws of Mauritius.

1.0 Policy Overview and Legal Context

Mevora Capital (the "Company") is legally obligated to adhere to the anti-money laundering statutes of Mauritius, including the Financial Intelligence and Anti-Money Laundering Act (FIAMLA) 2002 and its subsequent regulations. This manual outlines the mandatory procedures for all personnel to prevent the laundering of criminal assets, the funding of terrorism, and the financing of weapons of mass destruction.

All employees must familiarize themselves with these protocols and the Company's Customer Due Diligence (CDD) policies. This document should be utilized alongside the more comprehensive AML Handbook issued by the Financial Services Commission (FSC). The FSC uses this handbook as a benchmark to evaluate whether a financial institution's risk-based systems are effective and compliant.

Leadership Responsibilities

The Board and senior management are tasked with ensuring that internal controls are robust enough to prevent the business from being exploited for financial crimes. They must maintain documented systems that:

- Perform comprehensive risk assessments on the business and its clientele.
- Verify the true identities of customers and their ultimate beneficial owners.
- Confirm the intended nature and commercial logic of the business relationship.
- Maintain accurate and current identification data.
- Monitor transactions continuously, specifically flagging large, complex, or unusual patterns that lack a clear lawful purpose.
- Audit actual account activity against expected behavior.
- Heighten scrutiny for high-risk relationships.
- Empower the Compliance Officer and Money Laundering Reporting Officer (MLRO) with sufficient resources and full access to data for investigating suspicious activities.

1.1 Understanding and Mitigating Risk

The Company utilizes a Risk-Based Approach (RBA) rather than a simple "tick-box" exercise. This allows resources to be focused where the threat is highest.

Defining Risk

Risk is evaluated through three lenses:

- **Threat:** The potential for a person or activity to cause harm.
- **Vulnerability:** Weaknesses in the business (e.g., specific products or delivery channels) that could be exploited.
- **Consequence:** The resulting damage, such as legal penalties or reputational ruin.

Mitigation Strategy

Once risks are identified, the Company implements controls to lower them to an acceptable level. While no system can eliminate 100% of risk, a well-documented RBA ensures the Company acts reasonably and focuses its efforts efficiently. Per Regulation 31, these risk assessments must be updated regularly to address any new deficiencies.

1.2 Barriers to Effective Compliance

The Company recognizes that human factors often undermine AML efforts. Employees must stay vigilant against:

- Management’s failure to prioritize corporate ethics.
- Junior staff feeling their suspicions are "too small" to report.
- Hesitation to screen high-value "VIP" clients.
- Pressure from external managers to bypass CDD for the sake of speed.
- A lack of resources or a "confidentiality" mindset that hinders reporting.

1.3 Corporate Commitments and Consequences

Failure to comply with AML laws can lead to severe regulatory fines, criminal prosecution, and the loss of the Company's operating license. To prevent this, the Company commits to:

- Appointing a dedicated MLRO.
- Providing comprehensive training on identifying and reporting suspicious activity.
- Ensuring "Anti-Tipping Off" protocols (never informing a client they are under suspicion).
- Conducting internal audits to measure procedural effectiveness.
- Maintaining detailed records for regulatory inspection.

> **Important Note:** Every employee has a personal responsibility to report suspicions to the MLRO. Any breach of these policies may result in disciplinary action, including immediate dismissal.

2.0 Corporate Governance and Financial Crime Prevention

2.1 Overview

Effective corporate governance creates the necessary framework for leadership to prioritize the firm’s interests and those of its stakeholders. It ensures that the Company remains compliant with all Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) mandates. A transparent and accountable governance structure is essential for fostering a trustworthy business environment.

2.2 The Role of the Board in Compliance

The Board of Directors holds ultimate responsibility for the Company's management. Because they are best positioned to assess the risks of Money Laundering (ML) and Terrorism Financing (TF), they must actively oversee and regularly update business risk assessments.

Key Board Obligations:

- **Strategy Development:** Formulate a formal AML/CFT strategy based on identified risks to protect the Company's local and international reputation.
- **System Documentation:** Clearly define internal controls, policies, and the specific duties of the Compliance Officer (CO) and Money Laundering Reporting Officer (MLRO).
- **Regular Reviews:** Evaluate the effectiveness of compliance measures at least once a year, or immediately following significant organizational changes.
- **Independent Auditing:** Maintain an autonomous audit function to rigorously test the firm's ML/TF defenses, as required by Regulation 22(1)(d).

- **Resource Allocation:** Ensure that compliance policies reflect the Company's size and complexity, including provisions for sample testing of internal controls.

2.3 Designated Officers

The following individuals have been appointed to lead the Company's financial crime defenses:

Role	Appointed Officer
Money Laundering Reporting Officer (MLRO)	_____
Deputy MLRO (DMLRO)	_____
Compliance Officer (CO)	_____

2.4 The Money Laundering Reporting Officer (MLRO)

In compliance with Regulation 26(1), the MLRO is a senior-level individual approved by the Financial Services Commission (FSC). This officer must possess the necessary authority, expertise, and direct access to the Board.

Core Responsibilities of the MLRO & DMLRO:

- **Internal Disclosure Management:** Act as the final point for internal suspicion reports and determine if an external report to the Financial Intelligence Unit (FIU) is necessary.
- **Liaison:** Serve as the primary contact for the FIU and FSC regarding investigations or compliance queries.
- **Advisory:** Provide guidance to staff on avoiding "tipping off" clients during an investigation.
- **Reporting:** Produce monthly and annual reports for senior management detailing identified risks and incidents.
- **Records:** Maintain comprehensive documentation of all disclosures and investigative actions.

The Deputy MLRO holds equivalent status and experience, assuming all MLRO responsibilities during their absence. Both must be provided with sufficient time and resources to perform their duties effectively.

2.5 The Compliance Officer (CO)

The CO is a senior management figure responsible for the day-to-day oversight of the AML/CFT program. They ensure the Company remains in constant alignment with the FIAMLA, FIAML Regulations, and the FSC Handbook.

Specific Duties of the CO:

- Designing and maintaining internal compliance manuals and systems.
- Reporting instances of non-compliance directly to the Board.
- Monitoring the ongoing effectiveness of the AML/CFT program.

Board Support for the CO:

The Board must guarantee that the CO has unrestricted access to Company records, the full cooperation of all staff, and direct communication channels to the Board to ensure statutory obligations are being met.

> **Note:** The MLRO, DMLRO, and CO must all meet "Fit and Proper" standards, demonstrating high integrity, professional competence, and financial stability.

2.6 Key Terms and Definitions

Abbreviation	Full Term
AML/CFT	Anti-Money Laundering and Countering of Terrorism Financing
CDD / EDD	Customer Due Diligence / Enhanced Due Diligence
FSA / FSC	Financial Services Act 2007 / Financial Services Commission
FIAMLA	Financial Intelligence and Anti-Money Laundering Act 2002
FIU	Financial Intelligence Unit
Handbook	FSC AML/CFT Handbook 2020
STR	Suspicious Transaction Report
NRA	National Risk Assessment

2.7 Definitions and Procedures for Financial Crimes

2.7.1 Money Laundering (ML)

Under Part II of FIAMLA 2002, money laundering is the process of masking the illegal origins of criminal proceeds to make them appear legitimate. Criminals aim to hide the source, location, and true ownership of these assets. This applies not only to organized crime or drug trafficking but to any individual handling benefits derived directly or indirectly from criminal acts.

Money laundering generally follows a three-stage model:

- **Placement:** Introducing "dirty" money or illegal property into the formal financial system.
- **Layering:** Executing complex tiers of transactions to obscure the audit trail and distance the funds from their criminal source.
- **Integration:** Re-introducing the now-laundered funds into the economy as "clean" capital.

The Company is particularly susceptible during the Layering and Integration phases. By disguising ownership and changing the form of the assets, criminals seek to enjoy the fruits of their crimes—such as fraud, bribery, or smuggling—without triggering regulatory red flags.

2.7.2 Terrorist Financing (TF)

Terrorist Financing involves providing financial support to individuals or groups who plan or execute acts of terrorism. Unlike money laundering, the source of funds for TF can be either legal (e.g., personal savings or employment income) or illegal (e.g., drug sales or fraud).

The primary focus of TF prevention is the intended use of the funds rather than just their origin. The process typically involves:

- **Collection:** Gathering funds through donations, diverted charity money, or criminal acts.
- **Transmission:** Pooling and moving the funds to a terrorist entity.
- **Usage:** Utilizing the money for training, logistics, propaganda, or attacks.

Key Comparisons:

- **Difference:** ML usually happens after a crime is committed to hide the past; TF is often conducted to facilitate future illegal acts.
- **Similarity:** Both require the use of the formal financial sector to move value, and both often involve criminal networks.

2.8 The Global and Economic Impact

The exploitation of financial systems by criminals reduces global safety and creates severe consequences, including:

- **Reputational Loss:** Being viewed as a "safe haven" for criminals drives away legitimate investors.
- **Market Distortion:** Fair competition is destroyed by "front companies" funded by illegal wealth.
- **Institutional Instability:** Banks may become overly reliant on criminal deposits, leading to instability, fines, and legal costs.
- **Social Costs:** Increased government spending on law enforcement and healthcare due to related crimes like drug addiction.

2.9 Financing the Proliferation of Weapons of Mass Destruction (WMD)

Proliferation financing involves the transfer of goods, technology, or expertise used to develop nuclear, chemical, or biological weapons and their delivery systems. Support networks often use the international financial system to hide these transactions behind legitimate-looking front companies or middle-men.

3.0 Implementing the Risk-Based Approach (RBA)

3.1 Strategy and Statutory Duties

In accordance with Sections 17 and 17A of FIAMLA, the Company must actively identify, evaluate, and mitigate its specific ML and TF risks. An RBA ensures that the intensity of the Company's controls is proportional to the level of risk identified.

Core Obligations:

- **Risk Identification:** Analyzing threats based on customer profiles, geographic locations, product types, and delivery channels.
- **Risk Appetite:** Determining the level of risk the Company is willing to accept to meet its objectives, informed by the Mauritius National Risk Assessment (NRA).
- **Proportionality:** Applying "Enhanced Due Diligence" to high-risk scenarios while keeping measures cost-effective for lower-risk areas.

3.2 Procedural Steps for Risk Management

To fulfill the RBA mandate, the Board and management must follow these steps:

- **Pinpoint Threats:** Identify where the business is most vulnerable to exploitation.
- **Evaluate Impact:** Assess how likely a threat is to occur and the potential damage it could cause.
- **Implement Mitigations:** Create policies and controls to reduce these risks.
- **Manage Residual Risk:** Address any remaining risks that cannot be fully eliminated.
- **Continuous Monitoring:** Regularly update procedures to reflect changing criminal tactics.

Final Note: While no system is foolproof, a well-documented RBA balances the operational costs for the Company and its clients with a realistic, high-impact defense against financial crime. Comprehensive documentation is mandatory to prove compliance to the authorities.

3.3 Components of Business Risk

Risk is determined by analyzing the interplay between three core elements:

- **Threat:** Any entity or action with the capacity to inflict harm.

- **Vulnerability:** A weakness or opening that a threat can use to facilitate illegal activity.
- **Consequence:** The legal, economic, or social damage resulting from ML/TF.

To proactively block these risks, the Company must identify its specific threats by reviewing FSC and FIU notices, regulatory reports, media coverage, and internal data. This analysis informs the creation of targeted controls to close any gaps in the business. Proper documentation of this framework proves accountability and demonstrates how the Company monitors and refines its defenses.

3.4 Cumulative and Operational Risks

Risk factors should not be viewed in isolation. The Company must evaluate them holistically, as the combination of several minor factors may significantly increase (or decrease) the total risk exposure.

Beyond standard client risks, the Company must account for operational factors, such as the use of web-based platforms, which introduce specific vulnerabilities like cybercrime and identity fraud.

3.5 Risk Weighting and Scoring

The Company may assign different "weights" to risk factors based on their relevance to a specific transaction or relationship. For example, a client's geographical location might be weighted less heavily if the specific product they are using has very limited utility for money laundering.

Rules for Weighting Risk:

- No single factor should disproportionately dictate the final score.
- Profitability or economic gain must never influence a risk rating.
- Weighting cannot be used to "math away" high-risk classifications; it must remain possible for clients to be rated as high-risk.
- **Statutory High-Risk Scenarios:** Per Regulation 12(1), certain factors (like PEPs or suspicious activity) automatically trigger high-risk status and cannot be overridden by internal weighting.
- **Manual Overrides:** While the Company uses a weighted scoring model (see Annex A), staff may override automated scores if there is a documented, rational justification. If using third-party software for scoring, the Company must fully understand the underlying logic to ensure it aligns with regulatory expectations.

3.6 The Business Risk Assessment Process

The Business Risk Assessment (BRA) is a mandatory, cyclical process. It is not a "one-time" task; it must be reviewed at least annually or whenever the business undergoes significant changes (e.g., new products, new laws, or emerging economic trends).

Roles and Responsibilities

- **First Line of Defense:** The business units and management are responsible for the quality and execution of risk analysis, as they are closest to the activity.
- **Compliance:** Facilitates the process, monitors progress, and tests the effectiveness of controls.
- **The Board:** Holds ultimate legal responsibility for the BRA.

Key Assessment Areas

Per Section 17(2) of the FIAMLA, the BRA focuses on six primary pillars:

- **Nature and Scale of Activities:** Assessing how business volume, outsourcing, and organizational structure might be exploited.
- **Product and Service Vulnerabilities:** Identifying risks in specific offerings, such as those involving high cash volumes, virtual assets, or anonymous payment methods.

- **Delivery Channels:** Evaluating the risks of non-face-to-face relationships or the use of third-party introducers and intermediaries.
- **Customer Profiles:** Analyzing the location, complexity, and nature of the clients' own business activities.
- **Third-Party Reliance:** Assessing the risk of depending on external parties for Due Diligence.
- **Technology:** Considering how new technological developments might create new avenues for financial crime.

Geographic Considerations

The Company must evaluate the AML/CFT strength of the jurisdictions where it operates. High-risk countries are identified via:

- Mutual Evaluation Reports from the FATF or regional bodies.
- IMF and Financial Sector Assessment Programs.
- FATF lists of non-cooperative jurisdictions.

Note: Simply being a member of the FATF does not automatically guarantee a country has a robust or effective regime.

3.6.3 Customer Profiles and Service Delivery

The Company must evaluate threats based on the specific "who" and "how" of service provision:

- **High-Risk Personas:** Certain clients naturally carry higher risk, such as Politically Exposed Persons (PEPs), High Net Worth individuals, and those linked to high-risk territories.
- **Service Risks:** Vulnerabilities increase when dealing with high-value transactions, unlimited third-party funding, or payments made to third parties without prior Due Diligence.
- **Delivery Speed:** Rapid transaction processing or instant service delivery can be exploited to bypass scrutiny.
- **Non-Face-to-Face (NFTF):** Conducting business remotely significantly heightens risk, especially when combined with other factors like PEP status or high-risk jurisdictions.

3.6.4 Evaluating Customer Activities and Locations

The Company must analyze the scale and nature of a client's business operations, focusing on:

- **Industry Vulnerability:** Sectors prone to bribery or corruption (e.g., oil, gas, construction, or defense) require closer inspection.
- **Geographic Factors — TF Risk:** Assessing if a country is known for supporting terrorism, hosting extremist groups, or is under UN/EU financial sanctions or embargoes.
- **Geographic Factors — ML Risk:** Utilizing credible sources (e.g., Transparency International's Corruption Perceptions Index or UNODC reports) to identify regions with high rates of organized crime, fraud, or weak judicial systems.
- **Structural Complexity:** Intricate legal setups, opaque beneficial ownership, or a high volume of Non-Profit Organizations (NPOs) can be used to mask the true flow of funds.

3.6.5 Reliance on Third Parties

Under Regulation 21, the Company may allow third parties to introduce business or conduct CDD, provided:

- **Due Diligence on the Third Party:** The Company must verify the third party's reputation, the quality of their regulatory history, and their adherence to FATF-equivalent standards.

- **Information Chains:** It must be clear who met the customer in person and how that data is transmitted.
- **Contractual Compliance:** Third parties must agree to provide identification data immediately upon request. The Company remains ultimately responsible and must periodically test the third party's procedures.

3.6.6 Technology and Innovation

Per Section 17(3) of the FIAMLA, the Company must assess ML/TF risks whenever adopting new business practices or technologies (e.g., cloud storage, electronic verification, or virtual currencies).

- **Operational Risks:** Deficiencies in system integrity or over-reliance on external tech providers can lead to failures. Rapid tech shifts may also outpace staff expertise.
- **Reputational Risks:** Failures in data collection or high-profile AML breaches due to faulty tech can result in severe public backlash.
- **Legal Risks:** Remote access may make traditional crime detection difficult, potentially leading to non-compliance with Mauritius law.

3.7 Customer Risk Assessments (CRA)

A CRA must be completed before a relationship begins. It is a "living document" that evolves as more data is gathered.

The CRA Lifecycle:

- **Data Collection:** Gathering initial CDD.
- **Initial Evaluation:** Assigning a preliminary risk "bucket."
- **Verification:** Requesting further evidence based on the initial rating.
- **Finalized Rating:** Confirming the risk level and setting monitoring frequency.
- **Ongoing Review:** Continuous monitoring of transactions.

Key Principles:

- **High Risk ≠ Illegal:** A high-risk rating doesn't prove guilt; it simply mandates Enhanced Due Diligence (EDD).
- **No "Tick-Box" Mentality:** Assessments must be case-by-case or based on well-defined profile groups.
- **Automatic "High" Triggers:** Factors like PEP status, incomplete CDD, sanctioned country links, or "World Check" hits automatically move a client to the High-Risk category.

Review Frequency:

Customer Risk Level	Minimum Review Frequency
High Risk	Annually (or per transaction with high-risk regions)
Standard Risk	Every 3 years
Material Change	Immediate (e.g., client moves to a high-risk area)

Note: The Company policy is to review all clients annually, typically between January and February.

3.8 Core Risk Factors

The following pillars guide the risk assessment process:

Factor Category	Key Considerations
Customer Risk	Professional activity, public reputation, and observed behavior.
Country Risk	Geographic connections of the client and the beneficial owner.
Product/Service Risk	Level of anonymity (opaqueness), structural complexity, and transaction size.

Requirement: All risk classifications must be documented and objectively justified to ensure a clear audit trail for the FSC.

4.0 Customer Due Diligence (CDD) Framework

4.1 CDD Procedures and Implementation

To effectively combat money laundering and terrorism financing, the Company must verify the identities of all clients. This process, known as Customer Due Diligence (CDD), is the cornerstone of our AML/CFT strategy. We must identify and confirm the identity of every individual or entity involved in a business relationship, including directors, shareholders, beneficial owners, trustees, and those holding power of attorney.

4.1.1 The Necessity of Identification

Identification involves collecting personal details, while verification involves confirming those details using independent, reliable sources (such as a passport).

Why CDD is vital:

- **System Integrity:** It prevents the Company from being used as a tool for financial crime.
- **Law Enforcement Support:** It ensures accurate data is available for Suspicious Transaction Reports (STRs).
- **Risk Management:** It provides the data needed to identify and control high-risk relationships.

Core CDD Actions:

- Verify the identity of every applicant.
- Identify Beneficial Owners (the actual people who own or control the assets).
- Understand the commercial rationale and purpose of the relationship.
- Conduct ongoing monitoring to ensure transactions align with the known client profile.
- Keep all data current through regular reviews (more frequent for high-risk clients).

Important: If performing CDD is likely to "tip off" a customer that they are under suspicion, staff should stop the process and immediately file an STR.

4.1.2 Risk-Based Profiling

The Company uses a risk-based approach to determine the depth of CDD required. A client's profile—including their geography and business type—dictates how much information we collect and how strictly we verify it. While higher risk requires more scrutiny, a "high risk" label does not automatically imply criminal activity; it simply mandates more rigorous oversight.

4.1.3 Source of Funds (SoF)

SoF refers to the origin of the specific money or assets involved in a transaction (e.g., a specific bank transfer or investment).

- **Requirement:** Staff must assess the SoF for every account funding event using the Declaration of Source of Funds Form (Annexure C).
- **Evidence:** Clients must provide proof linking the origin of the money to its destination (e.g., bank statements or contracts).

4.1.4 Source of Wealth (SoW)

SoW refers to the client's total net worth and the activities that generated their overall wealth over time (e.g., inheritance, business profits, or investments).

- **High-Risk Requirement:** Detailed SoW verification is mandatory for all high-risk clients and Politically Exposed Persons (PEPs).
- **Evidence:** Clients must complete the Declaration of Source of Wealth Form (Annexure D). This info is cross-referenced with their CV and verified via audited accounts, statutory documents, or property deeds.

4.2 Identification and Verification Standards

The Company must follow documented steps to verify identities and determine if a client is acting on behalf of a third party. If a third-party relationship is unclear, an STR must be filed.

4.2.1 Natural Persons (Individuals)

We must collect and verify specific data for all individuals. For Standard Risk clients, one method of verification is usually enough. For High Risk clients, multiple methods are required.

Data to Collect	Verification Methods
Full Legal Name & Aliases	Valid Passport
Date & Place of Birth	National ID Card
Gender & Nationality	Valid Photo Driver's License
Residential Address (No P.O. Boxes)	Recent Utility Bill (within 3 months)
Employment Details / Public Office	Recent Bank/Credit Card Statement
Govt ID Number	Letter of Reference from a regulated bank

4.2.2 Legal Persons (Entities)

When the applicant is a company, partnership, or foundation, we must "drill down" through the layers of ownership to identify the Natural Persons who ultimately own or control the entity.

Verification hierarchy for entities:

- **Ownership:** Identify anyone with a controlling interest.
- **Control:** If ownership is unclear, identify who exercises effective control.
- **Management:** If neither above can be found, identify the Senior Managing Official.

Required Documentation for Entities:

- Certificate of Incorporation and Memorandum/Articles of Association.
- Registry Searches to confirm the entity is active and not being dissolved.
- Annual Reports or audited financial statements.
- Partnership Deeds or Foundation Charters.
- Certificate of Good Standing from a national regulator.

Note: If information is not available publicly, we must exercise extreme caution with client-provided data. Any third-party data providers used must be reputable and transparent about their verification methods.

4.2.3 Legal Arrangements (Trusts & Similar Entities)

For customers structured as legal arrangements, the Company must identify and verify the following beneficial owners:

- **Trusts:** The settlor, the trustee(s), the protector or enforcer (where applicable), the beneficiaries (or the specific class of beneficiaries), and any natural person who holds ultimate effective control, even if managed through a chain of ownership.
- **Other Arrangements:** Individuals holding roles equivalent to those mentioned above.

Verification Standards by Risk Level:

- **Low Risk:** Each required data point must be confirmed using at least one approved method.
- **Standard and High Risk:** Each data point must be confirmed using at least two independent methods whenever possible.

4.2.3.1 Data Requirements for Legal Arrangements

Subject	Data Points	Verification Methods
Principals	Individual data as per Section 4.2.1	See Natural Persons requirements
Legal Status	Legal form and date of creation	Trust Deed or equivalent instrument
Identity	Full legal name and trading names	Official Registration Certificate (if available)
Operations	Business nature and identifying numbers	Official registry or reliable third-party data
Location	Registered and mailing addresses	Principal place of business verification

Mandatory Assurances: Trustees or controlling individuals must provide written assurance that all data provided is complete and that they will notify the Company immediately of any changes.

4.3 Mergers and Customer Acquisitions

When the Company acquires a new block of customers or an entire business, it must conduct due diligence to ensure:

- The acquired business's AML/CFT framework aligns with current Mauritian law.
- The existing customer identification data is sufficient and risk-appropriate.

The Company may rely on inherited data only if the previous firm operated in a FATF-compliant jurisdiction and held complete records for every customer. If gaps are found, the Company must implement a prioritized remediation plan to update the files.

4.4 Authorized Representatives

When an individual is authorized to act for a client (e.g., via Power of Attorney or as an authorized signatory), the Company must:

- Verify the identity of the representative using the same standards as a primary applicant.
- Formally confirm their legal authority to act on the customer's behalf.
- Re-verify their identity if their authorization expires or their personal details change.

4.5 External Reliance (Third Parties)

Per Section 17D of FIAMLA, the Company may use third parties to perform certain CDD tasks, provided a formal contract exists. The third party must share all CDD info immediately and provide physical documents upon request. **Note:** The Company retains full legal responsibility for any compliance failures by the third party.

4.6 Digital Identity Verification

The Company may use electronic systems for onboarding natural persons but must first audit the system's reliability.

Security Measures for E-Verification:

- **Biometrics & Geotagging:** Using fingerprints, facial recognition, or location metadata to confirm the user's identity and presence.
- **Independent Corroboration:** Using multiple databases to cross-match data and checking documents against "stolen/missing" lists.
- **Tamper Checks:** Reviewing file types for digital manipulation and verifying the legitimacy of the sender's email.
- **Manual Oversight:** In high-risk cases, a lawyer or notary may be required to witness the digital onboarding process.

If the digital evidence is non-conclusive or appears fraudulent, the relationship must be blocked or terminated, and an internal disclosure should be made.

5.0 Enhanced Due Diligence (EDD)

Under Regulation 12, the Company must apply stricter "Enhanced" procedures for high-risk scenarios. EDD is mandatory for:

- PEPs (Politically Exposed Persons).
- Clients from High-Risk Jurisdictions with weak AML/CFT controls.
- Cases involving Suspicious Activity or the discovery of false identity documents.
- Any client identified as "High Risk" by the internal scoring model.

5.1 EDD Action Steps

When a relationship is flagged as high-risk, the following measures are required:

- **Management Approval:** Senior management must authorize the start or continuation of the relationship.
- **Wealth Verification:** Mandatory documentation and verification of the Source of Wealth (SoW).
- **Intensive Monitoring:** Real-time scrutiny of all transactions to confirm the destination of funds.
- **Frequent Screening:** Performing "World Check" and internet searches at least quarterly.
- **Payment Restrictions:** Requiring the initial payment to come from an account at a bank with equivalent AML standards.

> **Failure to Comply:** If the required EDD cannot be completed, the Company must terminate the relationship and file an STR with the FIU.

5.1 Politically Exposed Persons (PEPs)

Because of their positions of power and influence, PEPs carry a significantly higher risk of being involved in—or concealing—the proceeds of corruption and bribery. Consequently, identifying a PEP is a critical component of the Company's risk rating system, as these individuals receive a much higher risk score than standard clients.

Defining a PEP (Regulation 2 of FIAMLR 2018):

- **Domestic PEPs:** Individuals currently or formerly holding prominent public roles in Mauritius (e.g., Head of State, senior politicians, judicial or military officials, and executives of state-owned enterprises).
- **Foreign PEPs:** Individuals entrusted with similar prominent functions by a foreign government.
- **International Organization PEPs:** Senior managers or directors of international organizations (e.g., UN, IMF, World Bank).
- **Family & Associates:** The definition extends to family members (related by blood or marriage) and close associates (social or professional connections).

Company Mandate for PEPs:

- **Strict Verification:** Use PEP declaration forms (Annexure E) and screening tools like WorldCheck Refinitiv to confirm status.
- **Senior Approval:** Management must formally approve a PEP relationship before onboarding. If an existing client becomes a PEP, the relationship must be immediately reviewed for re-approval.
- **Mandatory EDD:** We must apply Enhanced Due Diligence to verify both the Source of Funds and the Source of Wealth.

5.2 Non-Face-to-Face (NFTF) Relationships

Relationships where the Company does not have physical contact with the customer—such as those established through electronic document submission or via trustees—present unique verification challenges.

- **Enhanced Measures:** If we cannot verify the authenticity of digital documents or have doubts about the identity of the person behind the screen, we must apply risk-sensitive EDD.

5.3 Connected Persons as PEPs

EDD requirements apply not only to the direct applicant but also to any connected persons, such as beneficial owners or controllers who are PEPs. The Company's policy on senior management approval and wealth verification remains identical for these underlying principals.

6.0 Simplified Due Diligence (SDD)

In specific, low-risk scenarios defined by Regulation 11, financial institutions may apply "Simplified" CDD. This does not mean ignoring CDD, but rather reducing the intensity of documentation (e.g., not requiring full beneficial ownership details for a company listed on a major stock exchange).

Key Constraints for SDD:

- **Justification:** The decision to use SDD must be documented, explaining why the risk is considered low based on the National Risk Assessment (NRA).
- **No Immunity:** SDD is strictly forbidden if there is any suspicion of money laundering or terrorism financing.
- **Ongoing Scrutiny:** Even under SDD, accounts remain subject to regular transaction monitoring.

Internal Policy Note: It is currently the Company's policy not to apply Simplified Due Diligence; we maintain a standard or enhanced level of checking for all clients.

7.0 Client Rejection Criteria

To protect the Company from legal and reputational fallout, we will refuse to onboard individuals or entities that present unacceptable AML/CFT risks.

Reasons for Rejection Include:

- **Opaque Business Models:** If the client cannot or will not explain their commercial activity.
- **Lack of Cooperation:** A refusal or reluctance to provide required KYC/CDD documentation.
- **Extreme Risk:** If the initial risk rating falls outside of the Company's risk appetite.

If a potential client meets any of these criteria, they should be rejected at the earliest stage. Staff should consult with the Board or Senior Management if there is any uncertainty regarding a high-risk applicant.

8.0 External Reliance and Introduced Business

8.1 Utilizing Third-Party Reliance

The Company may delegate specific Customer Due Diligence (CDD) tasks to qualified third parties, provided a formal contract is in place. Under Section 17D of the FIAMLA, while documents may be produced upon request later, the essential identification data must be transferred to the Company immediately during the onboarding phase.

Key Compliance Rules:

- **Ultimate Responsibility:** The Company remains legally liable for any CDD failures, regardless of third-party involvement.
- **Eligible Partners:** Third parties must be regulated, supervised, and compliant with record-keeping standards (Section 17F of the FIAMLA).
- **Geographic Risk:** We must evaluate the third party's location. Reliance is generally avoided if the third party is based in a "high-risk" jurisdiction or a country with strategic AML/CFT deficiencies identified by the FATF.
- **Scope of Reliance:** Third parties may only assist with identity verification and establishing the nature of the business. They are prohibited from performing ongoing monitoring or verifying the Source of Wealth/Funds.

Contractual Requirements:

To meet FSC standards, agreements with third parties (such as fund distributors) must:

- Explicitly state the third party's consent to be relied upon.
- Include clear obligations for the third party to maintain and provide records.
- Avoid "Secrecy" Clauses: The contract must not use conditional language like "subject to local law" that could prevent the Company from accessing CDD documents.
- Undergo regular assurance testing to ensure documents can be retrieved swiftly and are of sufficient quality.

8.2 Introduced Business

When a client is referred by an 'introducer' under Regulation 21, the Company must treat this as a high-stakes form of reliance:

• **Vetting the Introducer:** We must verify that the introducer is a regulated entity with AML/CFT procedures that meet Mauritian legal standards.

• **Written Assurances:** The Company must obtain a written guarantee that the introducer will perform the necessary CDD.

• **Data Access:** There must be a clear agreement that the Company has timely access to all original documents and that these records will be transferred to us if the introducer relationship ends.

• **Periodic Testing:** Senior management is responsible for regularly auditing these arrangements to confirm they remain robust.

9.0 Continuous Monitoring

9.1 The Two Pillars of Ongoing CDD

Maintaining a relationship requires more than just an initial check. Effective monitoring consists of:

• **Transaction Scrutiny:** Reviewing day-to-day activity to ensure it aligns with the client's known business and risk profile.

• **Relationship Maintenance:** Keeping CDD data current and periodically re-screening the client and their beneficial owners for new risks.

9.2 Monitoring Objectives

The primary goal is to identify and prevent financial crime by detecting "unusual" activity—transactions that lack a clear economic purpose or deviate from the client's established pattern.

Focus Areas:

• **Complexity:** Particular attention is paid to large, complex, or unusual transaction patterns.

• **High-Risk Flags:** Enhanced scrutiny is mandatory for PEPs, high-risk jurisdictions, and transactions involving massive cash volumes.

• **Peer Comparison:** Comparing a client's activity against similar customer groups to identify outliers.

9.3 Regulatory Obligations

Under Regulation 3(1) and Regulation 12, the Company is legally required to:

• **Keep Records Fresh:** Ensure all data and documents are updated, particularly for high-risk categories.

• **Verify Source of Funds:** Scrutinize transactions to ensure the money originates from legitimate sources consistent with the client's profile.

• **Enhanced Monitoring for PEPs:** Foreign PEPs and high-risk domestic PEPs require "enhanced" ongoing monitoring.

Examples of Enhanced Monitoring Techniques:

• **Increased Frequency:** Reviewing high-risk accounts more often than standard accounts.

• **Lower Thresholds:** Setting lower monetary limits for automatic alerts on high-risk accounts.

• **Independent Oversight:** Having the Compliance Officer (CO) or a non-involved party review high-risk transactions.

• **Management Information (MI):** Utilizing specialized IT systems to provide the Board with real-time data on risk exposure.

- **Deeper Insight:** Developing a comprehensive understanding of a high-risk client's personal circumstances through third-party data sources.

9.4 Monitoring and Management of PEP Relationships

The Company maintains a monitoring system designed to detect when an existing customer or beneficial owner attains Politically Exposed Person (PEP) status. This system distinguishes between foreign, domestic, and international organization PEPs.

9.4.1 Compliance and Approval Requirements

In accordance with Regulation 15(1)(b) of the FIAML Regulations 2018, the following protocols apply:

- **Foreign PEPs:** If a client or beneficial owner is identified as a foreign PEP during the relationship, senior management approval is mandatory to continue the business link, and Enhanced Due Diligence (EDD) must be applied.
- **Domestic/International PEPs:** The same senior management approval and EDD requirements apply if the relationship is categorized as "higher risk."
- **Research Proportionality:** While the Company is not required to perform exhaustive research on every remote family connection, the depth of research must be proportionate to the scale, complexity, and asset value of the relationship.

9.4.2 Ongoing PEP Surveillance

Because PEP status can change (e.g., a client takes office mid-relationship) or family members may be unaware of their status, the Company utilizes independent screening rather than relying solely on client disclosure.

Monitoring Standards:

- **Transaction Analysis:** All transactions are scrutinized to ensure they align with the client’s known Source of Wealth (SoW), Source of Funds (SoF), and original account mandate.
- **Documentary Evidence:** The Company may request invoices, bank statements, or agreements to verify the legitimacy of specific funds.
- **Quarterly Screening:** "World Check" and internet searches must be performed quarterly, with all results documented.
- **Annual Reviews:** All PEP files require a comprehensive annual review and formal approval by the Board or Senior Management.

Annual Review Checklist:

- Update and re-verify all KYC data.
- Re-confirm the relevance of EDD and the validity of SoF/SoW.
- Follow up on any previously noted adverse information (e.g., litigation or regulatory issues).
- Document a formal rationale for the decision to either maintain or terminate the relationship.

9.5 High-Risk Transactions and "Red Flags"

The Company remains vigilant in its duty under FIAMLA to detect Money Laundering (ML) and Terrorist Financing (TF). Indicators of high-risk activity include:

- Transactions that are unusual in size or frequency compared to the client’s peer group.
- Funds moving to or from atypical geographical locations.
- Sudden activity after a long period of account dormancy.

- Payments for "consulting" or "advisory" services that lack a clear business rationale.
- Donations to charities or political causes that seem out of character.
- Connections to jurisdictions known for high corruption or TF support.

Action Protocol: If a customer provides evasive answers or explanations that fail reasonable scrutiny, the Company will not execute instructions blindly. In such cases, a Suspicious Transaction Report (STR) must be filed, and legal counsel may be sought.

9.6 Cash Transaction Protocols

Cash carries a higher risk due to the lack of an audit trail. Per Section 5 of FIAMLA, it is an offense to make or accept cash payments exceeding 500,000 rupees (or foreign equivalent).

- **Enquiry:** Any proposed cash transaction outside of a client's normal pattern requires immediate investigation into the amount, currency age, and denomination.
- **Tax Evasion Risks:** Heightened scrutiny is applied to clients from jurisdictions where tax evasion is prevalent.
- **Disclosure:** If the legitimacy of a cash transaction cannot be verified, an internal disclosure is mandatory.

9.7 Transaction Monitoring Framework

The Company employs a manual system blending Real-Time and Post-Event monitoring:

- **Real-Time:** Conducted before a payment is processed using an internal bank transfer checklist.
- **Post-Event:** Monthly reviews to identify patterns that real-time checks might miss.
- **Business Plan Alignment:** Activity is compared against the client's filed projections. Material deviations require an updated business plan and potential EDD.
- **Oversight:** The Compliance Officer audits these processes to ensure all supporting documentation is present and aligned with the client's profile.

9.8 Manual vs. Automated Systems

The Company has determined that a manual monitoring process is appropriate given its current size and risk appetite. However, the following principles remain:

- **Risk-Based Parameters:** The frequency and depth of monitoring are dictated by the risk level of the relationship.
- **Human Alertness:** No system—automated or manual—replaces the "human element." Staff must use intuition and experience to recognize activities that lack economic common sense.
- **Audit Trail:** All decisions to discount alerts or "false positives" must be documented to maintain a clear audit trail.

9.9 Examination of Complex Transactions

Under Regulation 25(1), the Company must investigate the background of any transaction that is unusually large, complex, or lacks an obvious lawful purpose.

Examination Steps:

- Compare the activity against the existing Risk Assessment and KYC data.
- Make formal enquiries to find a rational explanation.
- Re-assess the client's risk rating based on the new findings.

• Document the entire examination to ensure it is "readily accessible" for auditors or the FSC/FIU.

9.10 Ongoing CDD and Data Maintenance

The Company performs ongoing Customer Due Diligence (CDD) to stay current with client developments.

• **Trigger Events:** Updated KYC is requested when a passport expires, a client's marital status changes, or a residential address is updated. For legal entities, changes in "connected persons" (controllers/owners) trigger a review.

• **Re-Verification:** Data is updated if the existing information is deemed inadequate for the current risk level or if its veracity is doubted.

• **Reporting:** All updated information from meetings or calls must be recorded and made available to the MLRO.

• **Annual Review:** Every client file undergoes a full annual review and a fresh Client Risk Assessment to ensure the integrity of the business relationship.

9.10.1 Customer Screening Protocols

During the initial onboarding (CDD) and throughout the relationship via ongoing monitoring, the Company performs comprehensive name-based searches. For corporate entities, screening extends to all beneficial owners, controllers, and beneficiaries. These searches utilize a combination of specialized risk management software and public domain data.

Negative Press & Adverse Media

Beyond checking PEP and Sanctions lists, the Company evaluates "negative press"—any adverse information, whether proven fact or unverified allegation. This ranges from formal criminal investigations reported in news outlets to fraud allegations made by third parties.

When assessing adverse media, the Company evaluates:

• **Credibility:** The reliability of the information source.

• **Severity:** The nature of the conduct alleged or proven.

• **Recency:** How long ago the event occurred.

• **Impact:** The potential reputational or legal risk to the Company by maintaining the relationship.

Documentation Requirements

In alignment with FSC expectations, the Company documents the following for every search:

• The specific source and date of the screening.

• The process used to confirm or discount a potential match.

• Full details of any negative press identified.

• Steps taken to verify or refute the claims (e.g., requesting client explanations).

• Any resulting risk-mitigation actions, such as reclassifying the client as "High Risk" or requiring additional Source of Wealth/Funds verification.

Screening Tools and Frequency

The Company employs a multi-layered screening approach:

• **Quarterly Manual Screening:** Performed for all clients via World-Check (Refinitiv).

• **Daily Automated Screening:** All clients are processed through Batch Risk Screen KYC 360 for real-time updates.

• **Scope:** Screening includes all stakeholders, directors, bank signatories, officers, and any other "connected persons" associated with the client.

9.10.2 Internal Procedures for Screening "Hits"

When a screening result (a "hit") is identified against a client or connected person, the following workflow is triggered:

• **Identity Verification:** The file handler first determines if the hit is a "True Match" or a "False Positive" based on the client's specific details.

• **Materiality Assessment:** If the hit is a True Match, the handler assesses the seriousness of the report.

• **Critical Hits:** For serious matters (e.g., criminal or civil offenses), the Company requests the client provide formal documentation, such as case law summaries or outcome confirmations from involved legal counsel.

• **Minor Hits:** Less severe reports are investigated through independent research and direct client inquiries.

• **Disposition:** If the match is negative (False Positive), the hit is discounted. All findings and decisions are formally recorded in the client's file.

9.11 Sanctions Screening and Targeted Financial Sanctions

Sanctions are global mandates used to combat issues like terrorism and nuclear proliferation. It is a legal offense to engage in business with any individual or entity appearing on these lists.

Scope of Screening

The Company monitors local and international lists, including OFAC, the UN Security Council (UNSC), and the European Union (EU). These are integrated into the World-Check and KYC 360 systems. We also regularly consult the Financial Intelligence Unit (FIU) website for updates. This screening applies to all customers and, where feasible, suppliers.

Legal Obligations under the UN Sanctions Act 2019

Pursuant to Section 23(1) of the UN Act, the Company is strictly prohibited from dealing with the funds or assets of a "designated" or "listed" party. This prohibition includes:

• All assets owned or controlled by the party, regardless of whether they are linked to a specific threat.

• Assets held jointly or controlled indirectly.

• Funds derived or generated from the assets of a listed party.

• Assets held by parties acting on behalf of, or at the direction of, a listed party.

Prohibitions and Exceptions

• **Accrued Interest:** While assets are frozen, interest or contract payments due before the listing may still accrue but must remain subject to the freeze (Section 23(2)).

• **National Sanctions Committee:** In specific cases (e.g., UNSCR 2231), the Committee may authorize payments for prior obligations, provided they are not related to prohibited items and the UN has been notified 10 days in advance.

Mandatory Reporting and Penalties

• **Reporting Requirements:** Any person holding or controlling assets of a designated party must immediately notify the National Sanctions Secretariat. This notification must include details of the assets, the party's identity, and any attempted transactions (including sender/recipient info and the origin of funds).

- **Timeframes:** Positive matches on any designated list must be reported to the National Sanctions Secretariat within 24 hours.
- **Non-Compliance:** Failure to comply with freezing obligations is a severe offense. Conviction may result in a fine of up to 5 million rupees (or double the asset value) and a minimum of 3 years imprisonment.

Freezing Orders (Section 26)

The Secretary for Home Affairs may apply for an ex parte freezing order from a Designated Judge. Once granted, these orders remain in force as long as the party is designated. The Company is notified of such orders via public notices in newspapers or direct communication.

Contact Information

Notifications and reports must be filed using the official templates found on the National Sanctions Secretariat website or directed to:

National Sanctions Secretariat
Prime Minister's Office (Home Affairs)
4th Floor, New Government Centre, Port Louis
Email: nssec@govmu.org

9.12 Compliance Officer Oversight

The Compliance Officer (CO) must be fully integrated into the Company's monitoring framework. This includes having unrestricted access to all monitoring results and data outputs.

Key Responsibilities of the CO:

- **Reporting:** Regularly provide the Board with management information, including statistical data, Key Performance Indicators (KPIs), identified trends, and summaries of corrective actions taken.
- **Rectification:** Ensure that any detected gaps or weaknesses in the monitoring system are addressed and resolved without delay.

Board Oversight:

The Board is responsible for reviewing the efficiency and suitability of these monitoring processes. This occurs during the annual assessment of the Company's business risk profile, policies, and controls. The Board must ensure that the frequency and intensity of monitoring remain proportionate to the risks identified.

10.0 Reporting Suspicious Transactions & Law Enforcement Liaison

10.1 Defining Suspicious Transactions

Under FIAMLA, a transaction is considered "suspicious" if it meets any of the following criteria:

- It suggests the laundering of criminal proceeds or the financing of terrorism.
- It is unnecessarily or unjustifiably complex.
- It lacks a clear economic rationale or a lawful objective.
- The identity of the parties involved cannot be verified to the Company's satisfaction.
- It triggers suspicion for any other justifiable reason.

Note on "Transactions": This definition includes opening accounts, establishing fiduciary relationships, and—crucially—proposed or attempted transactions that were never completed.

10.2 Identifying Unusual Activity

In accordance with Regulation 28(2) of the FIAML Regulations 2018, any activity that seems "out of the ordinary" must be scrutinized. Unusual activity includes transactions that are:

- Exceptionally large or complex.
- Part of an atypical pattern with no obvious purpose.
- Cause for doubt regarding the client's identity or their "good faith."

Procedures for Unusual Activity:

- **Detailed Scrutiny:** Investigate the background and purpose of the activity.
- **Enhanced Due Diligence (EDD):** Apply EDD measures, provided that doing so does not "tip off" the customer.
- **Internal Disclosure:** Determine if the findings warrant a formal internal report to the MLRO.

10.2.1 Examples of Unusual Situations

The following scenarios often indicate a need for further investigation:

- **Lack of Rationale:** Instructions that serve no commercial or legitimate purpose.
- **Evasiveness:** Clients who are reluctant to provide CDD, source of funds, or details about their business.
- **Atypical Usage:** Using an account for a single transaction or a very short period when long-term use was expected.
- **Inconsistency:** Transfers involving high-risk jurisdictions that do not align with the client's profile.
- **Structural Anomalies:** Unnecessary use of offshore structures or routing funds through third-party accounts.
- **Unjustified Urgency:** Demands for immediate execution regardless of high fees or penalties.

10.3 Reporting Procedures & The MLRO

Under Regulation 27 and 28(1), the Company maintains strict internal reporting protocols to ensure a clear chain of command to the Money Laundering Reporting Officer (MLRO).

Internal Reporting Workflow:

- **Knowledge/Suspicion:** Any employee who knows or suspects ML/TF activity must file an "Internal Disclosure" with the MLRO.
- **Predicate Offenses:** Employees do not need to identify the specific crime being committed; a "reasonable suspicion" of illicit activity is sufficient.
- **MLRO Evaluation:** The MLRO assesses the internal report alongside all other available data.
- **External Reporting:** If the MLRO confirms the suspicion, an "External Disclosure" must be filed with the Financial Intelligence Unit (FIU) as soon as practicable.

10.4 Indicators and "Red Flags"

While the presence of a "red flag" does not always prove illicit intent, the following indicators require heightened vigilance:

Category	Indicator / Red Flag
Cash/Funds	Unusually large cash deposits/withdrawals; unexplained wire movements; bank drafts exchanged for foreign currency.

Category	Indicator / Red Flag
Behavioral	Reluctance to identify beneficial owners; inability to explain the reason for a transaction.
Activity Patterns	Accounts becoming active after being dormant; personal and business funds being blurred; holding multiple accounts without a clear reason.
Third Parties	Payments to or from unknown individuals; requests to pay insurance proceeds to an un-associated third party.
Lending/Insurance	Frequent early loan repayments; early surrender of insurance policies at a loss; "loans" from relatives that lack documentation.
High-Risk Links	Transfers to NGOs/charities with suspected ties to proscribed organizations; high-value asset turnover (buy/sell) with payment by cheque.

Final Rule: If an explanation for a transaction is not reasonable or legitimate, staff must prioritize the filing of a report over the execution of the customer's instructions. Failure to do so may be considered a failure in the Company's duty to prevent and detect financial crime.

10.5 Internal Reporting Protocols

Under Regulation 28(1) of the FIAML Regulations 2018, all employees have a statutory duty to report suspicious activity. These "internal disclosures" must be submitted promptly to the Money Laundering Reporting Officer (MLRO) or their Deputy using the Internal Disclosure Form (IDF) found in Annexure F.

Operational Standards:

- **Full Cooperation:** Staff must provide the MLRO with unrestricted access to all records. The MLRO does not need to prove a specific crime; "reasonable grounds for suspicion" are sufficient to act.
- **Urgency:** In time-sensitive cases, reports may be made verbally but must be followed immediately by a written IDF.
- **Consequences:** Failing to report a suspicion is a breach of FIAMLA 2002 and can lead to criminal charges. Interfering with the reporting process will result in internal disciplinary action.
- **MLRO Seniority:** The MLRO must hold a senior position with the necessary independence and authority to make unbiased decisions.

Internal Reporting Contact Details:

Role	Name	Email	Phone
MLRO	_____	_____	_____
Deputy MLRO	_____	_____	_____

Anti-Tipping Off Rules: Upon receiving a report, the MLRO will issue an acknowledgment including a formal warning against "tipping off." Informing a client they are under suspicion is a criminal offense punishable by a fine of up to 5 million rupees and 10 years imprisonment.

10.6 External Reporting (STRs)

The MLRO is responsible for evaluating internal disclosures to determine if an external Suspicious Transaction Report (STR) is required.

- **Submission Timeline:** Under Section 14 of FIAMLA, if the MLRO confirms the suspicion, the STR must be filed with the Financial Intelligence Unit (FIU) as soon as possible, and no later than 5 working

days after the Company becomes aware of the transaction.

- **GoAML Platform:** All external reports and supporting evidence are submitted digitally via the FIU's GoAML portal.
- **Client Reclassification:** Once an STR is filed, the Company must immediately update its internal registers to flag that client as "High-Risk."

10.7 Disclosure Registers

The Company maintains a dual-purpose register (which may be a single document if clearly segmented) to track all reports:

- **Internal Register:** Records the date, the reporting employee, the recipient (MLRO/DMLRO), and the location of supporting files.
- **External Register:** Records the date of the FIU filing, the person who filed it, and documentation links.

10.8 & 10.9 "Appropriate Scrutiny" of Unusual Activity

When activity is flagged as "unusual" but not yet "suspicious," the Company performs Appropriate Scrutiny. This involves a deep dive into the client's CDD, historical patterns, and any explanations provided.

Key Scrutiny Indicators:

- The client cannot provide a logical reason for the activity.
- The explanation lacks economic sense (e.g., frequent small transfers despite high fees).
- Documentation appears altered, fraudulent, or incomplete.
- Media searches reveal negative information or corruption allegations.

Scrutiny Best Practices:

- Use diverse data (social media, news, property registers) to verify stories.
- Identify if the client is acting as an agent for a third party.
- Compare current activity against historical patterns (e.g., checking if cash surges are seasonal).

Warning: If asking for more info might alert the client to an investigation, stop the CDD process and file an STR immediately.

11.0 Record Keeping Requirements

The Company ensures a comprehensive audit trail is maintained for at least 7 years after a transaction is completed or a business relationship is terminated.

Records to be Retained:

- **CDD Data:** Identity documents, business correspondence, and risk assessments.
- **Transaction Data:** Sufficient detail to "reconstruct" the transaction (amounts, currencies, dates, counterparty details).
- **STR Records:** Copies of all internal and external reports and the evidence supporting them.
- **Training Logs:** Dates, content, and attendance lists for AML/CFT training.

Compliance Note: Facilitating a transaction under a false identity or destroying required records is a criminal offense, carrying a fine of up to 1 million rupees and 5 years imprisonment.

12.0 Employee Recruitment, Screening, and Training

The Company recognizes that its staff are the first line of defense. Even the best systems fail if employees are not properly vetted or trained.

12.1 & 12.3 Employee Screening

Prior to hiring, the Company performs rigorous background checks, including:

- Verifying employment history and professional qualifications.
- Obtaining criminal record checks and regulatory references.
- Screening candidates against UN Sanctions lists (which is also performed periodically for existing staff).

12.2 & 12.4 Training Oversight and Methods

The Board is responsible for ensuring training is effective. Training is not a "one-size-fits-all" approach; it may include classroom sessions, exams, or digital modules.

- **Goal:** Every employee, regardless of seniority, must understand their personal role in protecting the firm.
- **Effectiveness:** The Board may require assessments or exams to ensure the material is understood.

12.5 & 12.6 Frequency and Content

- **Induction:** New hires must complete AML training before starting work. This is often a requirement for passing probation.
- **Annual Refresher:** All staff receive basic AML/CFT training at least once a year.
- **Specialized Training:** High-risk roles (Board, MLRO, front-line staff) receive additional, specific instruction.
- **Triggered Training:** Extra training is provided if laws change or new technologies/products are introduced.

Core Training Topics include:

- Current ML/TF trends and "typologies."
- The responsibilities of the MLRO and CO.
- How to identify PEPs and manage their risks.
- Penalties for "tipping off" and failing to report.
- Recognizing unusual transactions that deviate from a client’s known profile.

12.7.2 Training for the MLRO and Deputy MLRO

To maintain peak effectiveness, the MLRO and DMLRO must engage in continuous professional development, including active participation in industry associations and specialized conferences. Their training must be comprehensive, covering:

- **Legal Frameworks:** In-depth knowledge of Mauritius' AML/CFT laws and the international FATF 40 Recommendations.
- **System Design:** Developing and testing internal AML/CFT monitoring programs and control systems.

- **Risk Management:** Identifying vulnerabilities in specific products/services and recognizing current global money laundering trends.
- **Disclosure Management:** Validating internal reports, managing the external filing process with authorities, and maintaining a strict non-tipping-off policy.
- **Agency Liaison:** Establishing effective communication channels with law enforcement.

12.7.3 Training for the Compliance Officer (CO)

The Compliance Officer holds primary responsibility for the Company's adherence to the FIAMLA and FIAML Regulations 2018. The CO must receive advanced training focused on the oversight of the entire AML/CFT program. This includes the rigorous testing of internal policies and the technical aspects of monitoring and control systems.

13.0 Independent AML/CFT Audit

Under Regulation 22(1)(d), every financial institution is legally required to establish an independent audit function. This serves as a critical evaluation tool to determine if the Company's policies and systems are effectively mitigating the specific risks identified.

13.1 Audit Scope and Strategy

The audit must be risk-based and acts as the Company's final line of defense. The scope typically includes verifying:

- Internal Risk Assessments and policies.
- The effectiveness of the MLRO and Compliance Officer functions.
- The integrity of CDD and Enhanced Due Diligence (EDD) measures.
- Compliance with record-keeping, training, and Sanctions obligations.
- The efficiency of transaction monitoring and suspicious activity reporting.

13.2 Requirements for Audit Professionals

The auditor (whether an individual or a firm) must be entirely independent. They cannot have been involved in creating the Company's risk assessment or implementing its AML program. The professional must possess:

- Relevant qualifications and specific expertise in the financial services industry.
- A thorough understanding of FIAMLA and its regulations.
- The ability to provide actionable recommendations for improvement.

The Board shall appoint an independent third party annually (or as otherwise decided by the Board) to conduct this review.

14.0 Additional Operational Requirements

14.1 Assurance and Testing

The Company adopts a risk-based approach to testing its lines of defense. This includes allocating specific resources for compliance audits and performing quarterly reviews of all client files to ensure they meet current standards.

14.2 Client Agreements

All new business applicants must sign a formal Client Agreement that explicitly includes clauses regarding AML/CFT compliance and obligations.

14.3 Document Certification Standards

The Company only accepts original documents or high-quality certified copies. Authorized certifiers include:

- Legal professionals (Lawyers, Notaries), Actuaries, or Accountants.
- Members of the Judiciary, Senior Civil Servants, or high-ranking Police/Customs officers.
- Diplomatic staff (Embassies/Consulates).
- Directors of regulated financial firms in equivalent jurisdictions.
- Commissioners of Oaths.

Note: Company employees may certify documents as "true copies" if they have personally sighted the originals during a face-to-face meeting.

14.4 Internal Registers

The Company maintains dedicated registers for:

- Breaches (Regulatory or Policy).
- High-Risk Clients.
- Politically Exposed Persons (PEPs).

14.5 Verification and Search Tools

To ensure robust screening, the Company utilizes:

- **World-Check & KYC 360** for comprehensive backgrounding.
- **OFAC & UN Sanctions Lists** for financial restrictions.
- **Web Checks & Transparency International (CPI)** for broader risk context.
- **FATF & OECD Lists** to identify high-risk jurisdictions.

14.6 Functional Delegation

The Board may collaborate with a licensed management company for various AML/CFT functions. While the Company may utilize the management company's tools, it retains the right to use its own. Regardless of the tools used, the Company conducts an independent audit at least once a year to verify the effectiveness of these outsourced or shared systems.

Appointed Management Company: _____

14.7 GoAML Registration

In compliance with FIU requirements, the Company, its MLRO, and its DMLRO are officially registered on the GoAML platform. This registration is current and active for all required reporting.

List of Annexures

- **Annexure A & B:** Business and Client Risk Assessment Criteria.

- **Annexure C & D:** Declarations of Source of Funds and Source of Wealth.
- **Annexure E:** PEP Disclosure Form.
- **Annexure F:** Internal Disclosure Form (for reporting to the MLRO).