ANTI-MONEY LAUNDERING PROCEDURES

OF VANEX LIMITED

Prepared in April 2019

[Last Updated April 2026]

CONTENTS

PART I

DEFINITIONS, POLICY STATEMENT AND INTRODUCTION

1.1. Definitions used in the text and their interpretations

The following words and expressions have the following meanings:

"Act"	The Anti Money Laundering and counter financing of Terrorism (AML/CFT)
"AML/CFT Act"	Anti-Money Laundering and Anti-Terrorism Financing Act 2001 (AMLATFA)
"The Company"	VANEX Limited
"VFSC"	Vanuatu Financial Services Commission
"VFIU"	Vanuatu Financial Intelligence Unit
"MLRO"	Money Laundering Reporting Officer
"Relevant Employee"	An employee is a relevant employee if, at any time in the course of his / her duties, he / she may have access to any information that may be relevant in determining whether a person is engaged in money laundering.

1.2. Policy Statement

a] The policy of the Company – The Company is taking security measures and has adopted policies, practices and procedures that promote high ethical and professional standards and prevent the Company from being used, intentionally or unintentionally, by criminal elements.

b] The directors, officers and employees of the Company shall at all times make every effort to maintain the highest standards of ethics, integrity, and prudence in the Company's operation and administration so as to ensure that the Company creates and maintains a good reputation and standing.

c] The directors, officers and employees shall at all times act in such a manner as to preserve the reputation of Vanuatu as a major international financial center and to prevent the use of the jurisdiction for illegal, criminal and terrorist purposes.

d] The anti-money laundering policies and procedures to be adhered to by the Company are contained in this manual including any amendments thereto.

e] Where any issue or matter is not addressed by this manual, guidance is to be sought from the anti-money laundering legislation referred to in Art. 1.1 above.

1.3 Introduction

Money laundering is a process of creating the appearance that money obtained from illicit means, such as drug trafficking or terrorist activity, originated from a legitimate source. The laundering of money is achieved by the placement of the money launderer's cash into the financial system, by creating complex layers of financial transactions to disguise the origin of the assets and by integration of the laundered proceeds into the economy as legitimately derived funds.

The prevention of money laundering in Vanuatu is governed by AML&CTF Regulation Order No. 122 of 2014 , AML and CTF Amendment Regulation No. 153 of 2015 and Anti-Money Laundering and Counter-Terrorism Financing Act No. 13 of 2014 as emended [also known as the AML & CTF [Amendment] Act No.16 of 2017]. These documents were made available to all staff members. Staff is required to review the information contained in these documents as well as these internal guidelines at least quarterly.

There is a wide range of methods that can be used to launder the proceeds of criminal activity, from purchase and resale of expensive assets to more complex schemes, which may involve money passing through networks of companies.

In general terms, money laundering is defined as the process of converting money/property, which is derived from illegal activities to give it a legitimate appearance. There are 3 stages in money laundering, which are:

- *Placement* – The physical disposal of cash proceeds derived from illegal activities;
- *Layering* – Separating the illicit proceeds from their sources through transactions that disguise the audit trail and provide anonymity;
- *Integration* – Integrating the laundered proceeds into the economy as normal funds.

PART II
GENERAL AND SPECIFIC PROVISIONS

2.1. General provisions concerning money laundering

Both individual employees and the Company itself are liable for criminal conduct if any of the offences below are charged by authorities. Money laundering offences can be distributed as follows:

a. *Arrangements relating to criminal property* – it is an offence to enter into arrangements which will facilitate acquisition, retention or use of criminal property. It is a defense that the employee reported his knowledge or suspicion to the law enforcement agencies via internal reporting procedures at the first available opportunity.
b. *Tipping off* – it is an offence to disclose information which is likely to prejudice an investigation either to the person who is the subject of a money laundering suspicion or any person other than the law enforcement agencies.
c. *Acquisition, use or possession of criminal property* – it is an offence to acquire, use or possess criminal property.
d. *Handling the proceeds of corruption* – corruption by government leaders and public sector officials inevitably involves serious crimes. Not only is there a major reputational risk in handling proceeds from such activities, but criminal charges and constructive trust suits can arise.
e. *Failure to report* – it is an offence for a person who knows or suspects or has reasonable grounds for knowing or suspecting that another is engaged in money laundering not to report such knowledge or suspicion as soon as reasonably practical to the authorities via internal reporting procedures.

2.2. Client confidentiality

It is important to stress out that the reporting of your suspicion of money laundering does not constitute a breach of client confidentiality.

2.3. Specific money laundering provisions for conducting the regulated activities

The following points apply to the Company in order to facilitate recognition of suspicions of money laundering and reporting of the foregoing to the authorities and so that the Company may produce its part of the audit trail to assist in official investigation. In particular, the Company is obliged to:

a. Have procedures to *verify* the identity of new counterparties;
b. Have procedures for employees to *report* any suspicious transactions;
c. Have *record keeping procedures* relating to the identity of clients and transactions effected for them;
d. Responsibility of *ensuring* that employees are suitably trained and made aware of the above procedures and in the recognition and handling of suspicious transactions;
e. Appoint a senior person as a *designated MLRO* to whom reports of suspicious transactions are to be made. This person must be free to act on his/her own authority and to make further investigations to determine whether a suspicion can be discounted or must be reported. The MLRO will be able to delegate duties, but will be responsible for the activities of such delegates; and
f. Stress the employees of the Company the potential of personal liability as well as that of the Company for failure to observe any aspect of the Regulations.

2.4. Money Laundering Reporting Officer (or MLRO)

Initially, the Compliance Officer will be the Money Laundering Reporting Officer (herewith – MLRO). The MLRO is (please contact support) and the Secondary MLRO is (please contact support). The Secondary MLRO will assist the compliance officer/MLRO with duties and fulfil his duties during absences. The MLRO will have responsibility for oversight of its compliance with the VFSC's rules on systems and controls against money laundering. The MLRO will have a level of authority and independence with access to resources and information sufficient to enable him/her to carry out that responsibility. In case should the Company decide to segregate the responsibilities of the Compliance Officer from those of the Money Laundering Reporting Officer, this manual will be amended accordingly.

The MLRO's responsibilities are:

a. Acting as the appropriate person to whom a report is to be made of any information or other matter concerning an employee's relevant suspicions;
b. To report suspicions to the VFSC and VFIU as he/she considers appropriate;;
c. To liaise with and respond promptly to any relevant request for information made by the VFSC; and
d. To take reasonable steps to establish and maintain adequate arrangements for awareness and training.

Where MLRO is not available, his duties will be performed by Alternate Money Laundering Reporting Officer (AMLRO). At other times, AMLRO will be assisting MLRO and share the same responsibilities as him/her.

2.5. Compliance

Compliance with the Company's anti-money laundering procedures is of the utmost importance. Not only is it important to maintain the Company's integrity, but failure to comply may constitute a criminal offence and call into question whether or not the Company and the employee concerned is fit and proper to conduct the business for which the Company has been licensed. Failures by individuals to comply with the money laundering procedures set forth in this manual can therefore result in summary dismissal.

Compliance with the Company's anti-money laundering policies and procedures will be the responsibility of the Compliance Officer. Specifically, the Compliance Officer will be responsible for:

a] oversight of the Company's anti-money laundering policies and procedures including updating or amending such policies and procedures to conform with changes in the Regulations;
b] ensuring that all relevant employees are made aware of the anti-money laundering policies and procedures of the Company;
c] ensuring that all relevant employees are made aware of regulations in respect of anti-money laundering;
d] ensuring that all relevant employees receive training in the recognition and handling of transactions carried out by or on behalf of any person who is or appears to be engaged in money laundering;
e] ensuring that all new relevant employees receiving training as soon as practicable after their appointment;
f] ensuring that the employees, management and directors of the Company adhere to the policies and procedures set out in this manual

PART III

PROCEDURES AND OBLIGATIONS OF THE COMPANY

3.1. Duty on establishing business relationships

The Company may not carry out a one-off transaction or form a business relationship in the course of relevant financial business unless:

3.1.1. It has money laundering procedures in place, meaning:

1. identification procedures
2. record keeping procedures; and monitoring;
3. recognition of suspicious transactions;
4. internal reporting procedures and such other procedures of internal control and communication as may be appropriate for the purpose of forestalling and preventing money laundering;

3.1.2. It makes its employees aware of the statutory duties and of the Company's procedures; and

3.1.3. It maintains training procedures.

3.1.4. Media request – any request for a statement or information from the media or other source must be directed to the MLRO for handling.

3.2. Identification procedures

The Company must ensure as soon as reasonably practical after the first contact has been made, and in any event before transferring or paying any money out to a third party, that satisfactory evidence is produced or such other measures are taken as will produce satisfactory evidence of the identity of any customer or counterparty (an "applicant"). If a client appears to be acting on behalf of another person, identification obligations extend to obtaining sufficient evidence of that third party's identity.

Where satisfactory evidence is not supplied, the firm will not proceed with any further business and bring to an end any understanding it has reached with the client unless in either case the firm has informed VFSC. If there is knowledge or a suspicion of money laundering, it will be reported without delay as provided under these procedures to the MLRO.

3.2.1. Methods of Identification

The Company obtains all information necessary to establish to its full satisfaction the identity of each new customer and the purpose and intended nature of the business relationship. The extent and nature of the information depends on the type of applicant (personal, corporate, etc.) and the expected size of the account.

When an account has been opened, but problems of verification arise in the service relationship which cannot be resolved, the Company can close the account and return the money to the source from which it was received. While the transfer of an opening balance from an account in the customer's name in another organization subject to the same KYC standard will be considered, the Company follow its own KYC procedures. The Company can consider the possibility that the previous account manager may have asked for the account to be removed because of a concern about dubious activities.

3.2.2. Due Diligence

Client identification must be carried out as soon as reasonably practicable after first contact is made. As part of its obligation to exercise due diligence in customer identification, the Company must

confirm that the identity information which it holds for its customers remains fully updated with all necessary identification and information throughout the business relationship. The Company reviews and monitors on a regular basis the validity and adequacy of customer identification information in its possession.

Notwithstanding the above and taking into account the degree of risk, if it becomes apparent at any time during the business relationship that the Company lacks sufficient or reliable evidence [data] and information on the identity and financial profile of an existing customer, the Company will immediately takes all necessary actions using the identification procedures and measures to provide due diligence, in order to collect the missing data and information as quickly as possible and in order to determine the identity and create a comprehensive financial profile of the customer.

Furthermore the Company monitors the adequacy of the information held and identity and economic portrait of its customers when and where one of the following events occurrences: Conduct of a significant transaction that appears to be unusual and/or significant as against the usual type of trade and economic profile of the customer;

A significant change in the situation and legal status of the customer such as:

- Change of directors/secretary
- Change of registered shareholders and/or actual beneficiaries,
- Change of registered office
- Change of trustees
- Change of corporate name and/or trade name
- Change of main trading partners and/or significant new business
- A significant change in the operating rules of the customer's account, such as:
    - Change of persons authorized to handle its account,
    - Request for opening a new account in order to provide new investment services and/or financial instruments.

In case of customer transaction via internet, phone, fax or other electronic means where the customer is not present to verify the authenticity of his/her signature, or that is the person who actually owns the account, or is authorized to handle the account, the Company has established reliable methods, procedures and practices to control access to electronic means to ensure that deals with the actual owner or authorized signatory of the account.

Where the customer refuses or fails to provide the Company with the required documents and information for identification and creation of a financial portrait, before entering into the business relationship, or during the execution of an individual transaction without adequate justification, the Company will not proceed in a contractual relationship or will not execute the transaction and may also report it to the AML/CFT Supervisor. This can lead to a suspicion that the customer is engaged in money laundering and terrorist financing.

If during the business relationship the customer refuses or fails to submit all required documents and information, within reasonable time, the Company has the right to terminate the business relationship and close the accounts of the customer. The compliance department also examines whether to report the case to the AML/CFT Supervisor.

3.2.3. Individual customers

The identity will be established to the Company's satisfaction by reference to official identity papers or such other evidence as may be appropriate under the circumstances. Information on identity will include, without limitation: full name; date of birth; nationality; complete residential address. Identification documents must be current at the time of the opening.

Personal Customers details required:

1. True full name and/or names used
2. Current permanent address, including postal code
3. Date of birth
4. Profession or occupation

Names should be verified by reference obtained from a reputable source that bears a photograph, such as:

- Current valid full passport
- Government issued photo identification card

In addition to the customer's name verification, the current permanent address should be verified by obtaining any one of the following documents in original form:

- Copy of a recent utility bill
- Local tax authority bill
- Bank statement
- Checking a telephone directory
- Credit card monthly statement

In addition to the above, an introduction from a respected customer personally known to the Manager of the Company or from a trusted member of staff can assist the verification procedure. Details of the introduction should be recorded on the customer's file.

In addition:

- Where customer contact is face-to-face;
- Where address verification may be difficult, government issued photo identification must be obtained
- If in doubt seek to verify identity with a reputable credit or financial institution in the customers country of residence

Where customer contact is not face-to-face;

- Verification of identity and current address should be sought from a reputable credit or financial institution in the applicant's country of residence.

Accounts for Corporate Customers:

- Company searches, and other commercial enquiries to ensure that the applicant has not been or in the process of being dissolved, struck off, wound up or terminated.
- If changes to company structure occur or ownership occurs subsequent to opening of an account with the company, further checks should be made.
- Identity verification should aim to identify:
    - The company
    - The directors
    - All persons duly authorized to operate the account
    - In case of private companies, the major beneficial shareholders
    - The company's business profile in terms of nature and scale of activities

The following documents are required:

- The original or certified copy of the Certificate of incorporation
- Constitution
- Resolution of the Board of Directors to enter into transactions on the Forex market and conferring authority to those who will act for the customer
- Where appropriate a search of the file at the Companies' Registry
- Identity of individuals who are connected with the company

3.2.4. Corporate customers

Where the applicant company is listed on a recognized or approved stock exchange or where there is independent evidence to show that the applicant is a wholly owned subsidiary or subsidiary under the control of such a company, no further steps to verify identity over and above the usual commercial checks and due diligence will normally be required.

Where the applicant is an unquoted company, it will be subject to a procedure aimed to identify it, confirm its existence, good standing and authority of persons acting on its behalf. Documentation required for such purposes may change depending on each particular jurisdiction and will typically include:

a] Certificate of incorporation/certificate of trade or the equivalent, evidencing the company is indeed incorporated in a particular jurisdiction under the respective legislation;
b] Certificate of Incumbency or an equivalent document, listing current directors of the company
c] Statutes, Memorandum and Articles of Association or equivalent documents confirming the authority of the respective officers of the company to legally bind it and the manner in which this may be done.
d] Extract from the Commercial Register of the country of incorporation may also be used to confirm the aforementioned information, if such information is provided in the extract.

3.2.5. Beneficial Owners

Due diligence must be done on all principal owners identified in accordance with the following principles:

a] Natural persons: where an applicant is an individual, the Company must clearly establish, based on information and documentation provided by the client, whether the client is acting on his/her own behalf.
b] Legal entities: where the client is a company, such as a private investment company, the Company must understand the structure of the company, based on information and documentation provided by the client, sufficiently to determine the provider of funds, principal owner(s) of the shares and those who have control over the funds, e.g. the directors and those with the power to give direction to the directors of the company. The Company will request KYC documents on all beneficial owners with 15% or more ownership. If ownership amounts in less than 15%, KYC will be requested on discretion of MLRO.

While use of clear scanned versions of documents will be accepted and in case any further clarification is needed, attested scanned copies or original attested copies may be sought for.

The certifiers may be:
- a notary public or another authority with equivalent power to certify copies of documents in the relevant jurisdiction; or
- a relevant state official (judge, police officer, consular official, etc); or
- an authorized financial institution.

Copies of documentation may also be certified by the Company's staff, if these have been made in their presence.

If any document regarding the corporate entity (such as extract from the Commerce Register) is available online through an official website of the relevant state authority, the Company may refer to such online version of the document, provided that a printout is made by a staff member of the Company and stored in the respective client file.

The clients will also be asked to provide relevant contact details, such as phone number and e-mail address.

3.3. High- risk countries

The Company will apply heightened scrutiny to clients and beneficial owners resident in and funds sourced from countries identified by credible sources as having inadequate anti-money laundering standards or representing high-risk for crime and corruption. The Company will apply more stringent standards to the transactions carried out by clients or beneficial owners domiciled in such countries.

3.3.1. Offshore jurisdictions

Risks associated with entities organized in offshore jurisdictions are covered by due diligence procedures laid out in these guidelines. However, the Company will apply more stringent standards to the transactions carried out by clients or beneficial owners head-quartered in such jurisdictions.

3.3.2. High-risk activities

Clients and beneficial owners whose source of wealth is derived from activities known to be susceptible to money laundering will be subject to heightened scrutiny.

3.3.3. Public officials

Individuals who have or have had positions of public trust such as government officials, senior executives of government corporations, politicians, political party officials, etc. and their families and close associates will be subject to heightened scrutiny.

3.4. Verification responsibility

It is the responsibility of the MLRO to verify the identity of each new applicant when taking on a new client. The verification procedures must be completed and satisfactory evidence of the new applicant's identity must be obtained before the applicant is sent a customer agreement except in exceptional circumstances (as determined in writing by the Compliance Officer).

3.5. Verification procedures

The verification process should be documented by making a record of the relevant information on the Company's Client Identification Questionnaire.
If in doubt as to which information must be obtained to verify an applicant's identity staff must consult the MLRO for guidance without delay and prior to commencing any dealings.

3.6. Compliance Officer approval

Once completed, the Client Identification Questionnaire should be completed and signed by the employee or the person designated by the Company and must be handed over to the Compliance Officer for record keeping. For each applicant the Compliance Officer must also countersign the forms and will be responsible for deciding what further information, including documentation, is required prior to conducting business for the applicant.

3.7. On-going monitoring and recording of accounts and transactions

On-going monitoring is an essential aspect of effective KYC procedures. The Company can only effectively control and reduce the risk if it has an understanding of normal and reasonable account activity of its customers so that it has means of identifying transactions which fall outside the regular pattern of an account's activity. Without such knowledge, it is likely to fail in its duty to report suspicious transactions to the appropriate authorities in cases where they are required to do so. The extent of the monitoring needs to be risk-sensitive.

For all accounts, the Company has systems in place to detect unusual or suspicious patterns of activity. This can be done by establishing limits for a particular class or category of accounts. Particular attention is paid to transactions that exceed these limits.

Certain types of transactions alert to the possibility that the customer is conducting unusual or suspicious activities. They may include transactions that do not appear to make economic or commercial sense (big transactions), or that involve large amounts of cash deposits that are not consistent with the normal and expected transactions of the customer.

Intensified monitoring for higher risk accounts is conducted. The Company has set key indicators for such accounts, taking note of the background of the customer, such as the country of origin and source of funds, the type of transactions involved, and other risk factors.

3.8. Record keeping procedures

The Company is required to keep records for a period of at least 6 years by law. The 6 year period is calculated following the carrying out of the transactions or the end of the business relationship.

The following records must be kept:

- Copies of the evidential material of the customer identity.
- Relevant evidential material and details of all business relations and transactions, including documents for recording transactions in the accounting books and
- Relevant documents of correspondence with the customers and other persons with whom they keep a business relation.

All documents and information are available rapidly and without delay to the authorities for the purpose of discharging the duties imposed on them by the law. The AML/CFT Supervisor needs to be able to compile a satisfactory audit trail.

Document retention may be in original documents or certified true copies and be kept in hard copy, or other format such as electronic form given that they can be available at any time and without delay.

When setting up document retention policies, the Company considers the statutory requirements and the potential needs of the unit. Documents and information must be original or true copies. In cases where the documents are being certified by another person and not the Company, or the third party, then the documents must be notarized.

3.9. Education and training

Staff who handles or are managerially responsible for handling transactions which may involve money laundering will be made aware of:

3.3.4. their responsibilities under the Company's anti-money laundering arrangements, including those for obtaining sufficient evidence of identity, recognizing and reporting knowledge or suspicion of money laundering and use of findings of material deficiencies;
3.3.5. the identity and responsibilities of the MLRO;
3.3.6. the law and regulations relating to money laundering; and
3.3.7. the potential effect on the Company, its employees and its clients of any breach of money laundering provision. All members of staff will receive periodic training in addition to the information provided in this document. This is expected to include seminars organized by the Compliance Officer. Employees should ensure that they regularly update their knowledge of these procedures given the seriousness of the consequences of breaching the Anti-Money Laundering and Counter-Terrorism

Financing Act No. 13 of 2014, AML&CTF Regulation Order No. 122 of 2014, its amendments, this Anti-Money Laundering policy and other applicable regulations and acts.

A record of anti-money laundering training supplied must be maintained and will include the dates, nature and names of recipients of such training.

3.10. Duty to report

There is a statutory and regulatory obligation on all staff to report information which comes to their attention, which gives rise to knowledge or suspicion or reasonable grounds for knowledge or suspicion of money laundering. Thus, even if a member of staff does not actually know or suspect but reasonably should have known or suspected, and does not report, he/she would be committing an offence. To this end, continuous surveillance for suspicious transactions must be carried out. Knowing its customers is the Company's most important line of defense in preventing or detecting money laundering activities. It is important that the Company verifies the identity of new counterparties and ensures that they are involved in bona fide business activities and that they share the Company's high standards of integrity and business practice.

Knowledge in relation to money laundering has been in the past defined widely and includes: willfully ignoring the obvious, willfully and recklessly failing to make inquiries as a reasonable and honest person would make, knowledge of circumstances which would indicate facts to such honest and reasonable person or put them on enquiry.

Suspicion is assessed on a subjective basis; however it goes beyond mere speculation.

Reasonable grounds to suspect introduces an objective test rather than a subjective test of suspicion. It might therefore include willful blindness (i.e. turning a blind eye to the obvious), negligence (recklessly failing to make adequate enquiries) and failing to assess adequately the facts and information presented or available.

The Company will therefore ensure that staff takes all reasonable steps in the particular circumstances to know the customer and the rationale for the transaction or instruction.

3.11. Suspicious transactions

A suspicious transaction will often be one which is inconsistent with a customer's known legitimate business. Emphasis will therefore be placed on knowing the customer's business and his/her requirements. It is the responsibility of all staff to report knowledge or suspicion of money laundering.

The following questions may help to determine whether a transaction is suspicious:

- Is it inconsistent with the client's known activities?
- Is the size of the transaction inconsistent with the normal activities of the client, or the client's net worth, as determined at the initial identification stage?
- Are there any other transactions linked to the transaction in question of which the Company is aware and which could be designed to disguise money and divert it into other forms or other destinations or beneficiaries?
- Is the transaction rational for the client?
- Has the client's pattern of transactions changed?
- Is the client's proposed method of payment unusual?

Suspicions of money laundering, however minor, should be discussed immediately with the MLRO. An internal form for making a report of a suspicion or knowledge of money laundering has been included in this manual.

The MLRO is required to report to VFSC where a report of knowledge or suspicion has been made.

Steps should also be taken to monitor accounts held on behalf of customers that hold positions of public trust such as government officials, politicians and any known connected accounts.

3.12. Confidentiality

Reporting a suspicion is a defense to a claim for breach of confidence. However, any statements to the press or other publicity must be routed through the MLRO or his deputy. Similarly, any requests for information or statements should be referred to him or his deputy for reply. Confidentiality whilst an investigation is ongoing is of the utmost importance and employees are reminded of the offence of "tipping-off".

3.12. Sanctions

Sanctions are measures/tools, mainly imposed by the United Nations (UNSC), Regional Bodies such as the European Union or by individual countries against a country, jurisdiction, regime, organization or individual believed to be violating, or threatening to violate, international law.

These sanctions impose restrictions on activities relating to particular countries, goods and services, persons and entities. Sanctions can take the form of a range of restrictive and/or coercive measures, targeting individuals, entities, organizations and governments. They can include but are not necessarily limited to:

- arms embargoes;
- travel bans;
- asset freezes;
- restrictions on the provision of services;
- increased vigilance of transactions and activities;
- reduced diplomatic links;
- reductions/cessation of any military relationship;
- flight bans and admission restrictions;
- suspension from international organizations;
- withdrawal of aid;
- trade embargoes; and
- restrictions on cultural /sporting links.

The aims of sanctions are:

> *'to limit the adverse consequences of the situation of international concern [for example, by denying access to military or paramilitary goods, or to goods, technologies or funding that are enabling the pursuit of programs of proliferation concern]; to seek to influence those responsible for giving rise to the situation of international concern to modify their behavior to remove the concern [by motivating them to adopt different policies]; and to penalise those responsible [for example, by denying access to international travel or to the international financial system].'*

The authority for Vanuatu to abide by Sanctions Laws imposed by the international community derives primarily from its membership to the United Nations under the Charter of the united Nations and relevant United Nations Security Council Resolutions.

To enable the Company to identify and prevent entering into or continuing in a relationship with a sanctioned target, the Company screens all customers against relevant sanctions lists (which include the United Nations Financial Sanctions Lists), before entering into a business relationship with them and on a regular and periodic basis following the establishment of the relationship.

Before a business relationship is established with a customer, the Company captures various personal details of the individual, these include:

- Name;
- Address; and
- Date of birth.

The Company then uses the software services of World Check, an external service provider who provides access to a wide range of data sources.

Whilst the wide range of sources increases the number of potential matches identified, this ensures that the risk of the Company accepting or continuing a relationship with a sanctioned individual is minimized.

Despite conducting ongoing screening, the Company recognizes that there is a residual risk that a breach of financial sanctions may occur during the period between re-screenings as a sanctions list may be updated during that time of a list being updated and a rescreen; however, considering the frequency of lists being updated, the Company considers this risk to be minimal and acceptable.

Considering the absolute nature of the sanction's regime (i.e. values and amounts are immaterial), where a potential sanctions match is identified through either the initial or the ongoing screening process, the Company ensures that the account is immediately frozen and the case is escalated to the AML/CTF Compliance Officer for immediate investigation, before determining the best course of action and the further steps to be taken, including establishing whether the match to a target is genuine.

Where it is determined that the match is a "false positive", precise records of the reasons for discounting the match are retained.

Where a positive match is identified, the AML/CTF Compliance Officer or AML Assistants immediately issue a company freeze notice and identifies the specific regime that the target is listed on and the requirements for dealing with such a match.

Following this investigation, the AML/CTF Compliance Officer may:

- seek guidance from an external party to determine the Companies requirements under alternative regimes and or investigate whether the person or entity being dealt with is in fact a target; AND
- where there is an applicable positive match:
    - MUST Submit a report within 5 days to the Sanctions Secretariat. The 5 days are calculated as of being notified of the designation; the date of publication of the designation in the Official Gazette; or coming into the possession of the property (whichever is sooner), AND
    - MUST Submit a separate report within 2 days of a suspicious transaction or activity, or a transaction involving terrorist property, in accordance with the Anti-Money Laundering and Counter Terrorism Financing Act No. 13 of 2014 (AML/CTF Act).

3.13. Audit Program

An annual AML audit serves as an integral part of our business by helping to protect us from being an unintentional conduit for money laundering and fraud. The audit is a systematic check of our AML/CFT risk assessment and our AML/CFT program by a suitably qualified person (the auditor). The end result is a written report on whether we meet the minimum requirements for our AML/CFT risk assessment and our AML/CFT program; The AML/CFT program is adequate and effective throughout a specified period; and whether any changes are required.

Audit of our AML/CFT Program includes whether it complies with all of the obligations in the Act; whether the policies, procedures and controls are based on the AML/CFT risk assessment; whether the policies, procedures and controls are adequate; and whether the policies, procedures and controls have operated effectively throughout the period.

A review of our AML & CTF Program will be undertaken at least annually also in case of important changes of legal acts. We will establish (or outsource to a third-party provider) an independent internal audit function to test our AML and CTF processes, procedures and systems. The review/testing will be undertaken either internally by a senior person independent from our AML & CTF Compliance Officers - for instance internal auditor - or by an external service provider that will be retained to conduct such review. In either event, the Auditor will be finally approved and accepted only by the Board of Directors of the Company.

The result of the review, including any report prepared, will be provided to the Board of Directors who is ultimately responsible, together with Compliance Officers, to interpret and develop key actionable items which will address all shortcomings identified by the audit – if any.

The results of the audit are stored indefinitely and are compared to previous years results. The comparison allows for key takeaways on the overall direction of the Companies AML/KYC compliance – whether it is getting better or deteriorating.

3.14. Internal reporting

Employees must report any relevant money laundering suspicions to the MLRO.

The suspicion should be fully documented, including the name and location of the reporting employee, full details of the client and the respective account, description of the information giving rise to the suspicion.

All internal enquiries made in relation to the report, and the reasoning for submission or non-submission of the report should also be documented.

The MLRO should remind the reporting employee to avoid "tipping off" the subject of the reported suspicion, and that information concerning a report should not be disclosed to any third parties.

The requirement to report also includes those situations where the business or transaction has not proceeded because the circumstances surrounding the application or proposal give rise to a suspicion of money laundering.

3.15. External reporting

The MLRO or his duly authorized delegate will consider the reported information, and where, following consideration, the suspicion remains, a report must be made to VFSC.

Any report made by the MLRO or his/her delegate will not be subject to the consent or approval of any other person.

In order to make this assessment, the MLRO will have access to any information, including "know your business information" in the Company's possession that could be relevant. Know your business information will include: information about the financial circumstances of a client or any person on whose behalf the client has been acting or is acting; and the features of the transactions which the Company has entered into with or for the client.

Internal Reporting form can be found in Appendix 1

Information about notification to the VFSC can be found in Appendix 2

INTERNAL REPORTING FORM

Instructions

All staff members are under an obligation to report knowledge or suspicions of money laundering in accordance with these procedures. An employee commits an offence if a reasonable ground for suspicion/knowledge of money laundering exists and he/she fails to report. Therefore, if you have a suspicion, no matter how small:

[a] Promptly inform the MLRO verbally and complete this reporting form. You are now absolved from any personal criminal liability for failing to report the suspicion. However, you must comply with the directions of the Compliance Officer and management in respect of the customer and transaction until the matter is resolved;

[b] You may not continue to manage process transactions on the customer's account until clearance is given by the Compliance Officer;

[c] The Compliance Officer must promptly review the situation with senior management;

[d] The review will either sustain or negate the suspicion. A sustained suspicion will lead to the Company making a confidential report to the authorities who will direct the Company on further steps to be taken;

[e] You must not tip-off the client or any other person that you or the Company has made a report;

[f] If in doubt, seek guidance from the Compliance Officer.

PLEASE COMPLETE THE FOLLOWING

1. *Your name:* _____

2. *Name of the customer:* _____

3. *Country of incorporation/origin:* _____

4. *Type of customer [please underline the appropriate type]:*

Corporation *Partnership* *Other*

5. *Name of contact:*
Position: _____
Contact details: _____
Telephone: _____
Facsimile: _____

6. *Is the customer an existing customer*

❑ Yes

❑ No *please provide all available identification information below*
_____

7. *Suspicion aroused or knowledge gained during identification procedure*:

[a] How was the customer introduced to us?
[b] Is verification of identity complete

[c] Has obtaining verification of the customer's identity been unusually difficult?

If yes please specify:
_____
_____

8. *Please detail in the space below the knowledge or suspicion[s] of money laundering, why you are suspicious and any other relevant information. Please give as much information as possible. The following points may be of assistance*:

[a] Is the role of any fiduciary involved in operation of the account usual?
_____
_____

[b] Is payment into the account effectuated by a third party without any apparent connection with the prospective investor?
_____
_____

[d] Other suspicious circumstances:

_____
_____

9. *MLRO: please add any further relevant information to support or negate the suspicion.*

Signed: **Date:**
MLRO

REPORTING TO VFSC

The company will be reporting to the VFSC [Vanuatu Financial Services Commission] for any suspicious activity or client. This can be a notification of the report made to the VFSC and in case the VFSC will require additional information, the Company will ensure all relevant, precise, complete and up-to date information is given to the VFSC or other relevant authorities.