ANTI MONEY LAUNDERING AND COUNTER TERRORISM FINANCING PROCEDURE MANUAL FOR BALTISEE LIMITED.

Table of contents

1. WHAT IS MONEY LAUNDERING?

1. **Definition:** Money laundering is a process of concealing the true origin and ownership of illegally obtained money. Principally, it is the precedent of criminal activities such as illicit drugs, corruption, organized crime, fraud, sex trade, forgery, illegal logging/fishing revenue evasion, counterfeit money, privacy terrorism etc.... which criminal attempt to disguise.

2. **Money laundering process:** There is more than one method of laundering money. Methods can range from purchase and resale of real estate or luxury items to passing money through a complex web of legitimate business and shell companies. In most cases, the proceeds of these criminal activities take the form of cash. There are three stages of money laundering, during which there may be numerous transactions made by launderers that could alert us.

3. **Placement:** Placement is the physical disposal of the cash or assistance derived from illegal activity. It includes the opening of numerous bank accounts, depositing cash, exporting cash, and using cash to purchase high value goods such as property or businesses.

4. **Layering:** Layering is The separation of criminal proceeds from their source of creating a complex layering process of financial transactions designed to defeat the audit trail and provide anonymity. It may include telegraphically transferring phones overseas, depositing cash overseas, and reselling goods previously with cash.

5. **Integration:** Integration provides apparent legitimacy to criminally derived wealth. If the layering process succeeds, integration schemes place the laundered funds back Into the economy so that they can enter the financial system appearing to be legitimate business funds. This may be achieved through a complex web of transfer or income from apparently legitimate business previously purchased with the proceeds of illegal activities.

2. WHAT IS FINANCING OF TERRORISM?

Terrorist financing involves collecting and providing funds for terrorist activity. The primary objective of terrorism is to intimidate a population or to compel a government or an international organization to abstain from doing any act. The goals of the terrorist or terrorist organization is to maintain financial support in order to achieve their aims, and the successful terrorist group, this one that is able to build and maintain an effective financial infrastructure.

Terrorists need finance for a wide variety of purposes -recruitment, training, travel, materials and setting up safe havens.

Terrorists control funds from a variety of sources around the world and employ sophisticated techniques to move funds between jurisdictions. In order not to be detected, a terrorist group draws in the service of banks and non banking institutions and takes advantage of their services products

6. Financing Terrorism and Associated activities
If a known terrorist organization conducts or seeks to conduct a transaction via the business (whether or not the transaction or proposed transactions involves cash), such transactions or proposed transactions are deemed to be a suspicious transaction and the business might submit to the international money laundering information network (MoLIN).

3. OUR POLICY

We are expected by the AML & CTF act to have in place adequate policies, practices and procedures that promote high ethical and professional standards and prevent the institution from being used, Intentionally or unintentionally, by money launderers and terrorism financiers.

BALTISEE LIMITED, has adopted an Anti-Money Laundering (AML) Compliance policy according to the international Money laundering information network (IMoLIN) standard. Based on the requirements of the above mentioned act, BALTISEE LIMITED, is committed to the maintenance of a compliance program which includes:

1. A system of internal controls and procedures to ensure ongoing compliance
2. Internal or external independent testing for compliance
3. Training of personnel in the identification of suspicious transactions and
4. Designation of an appropriate officer, responsible for continual compliance with the applicable laws.

The policies and procedures in this manual implement the duty of vigilance expected of us to avoid assisting the process of laundering and terrorism financing and to react to possible attempts at being used for those purposes.

1. Scope and objectives of policy

This policy applies to all BALTISEE LIMITED, officers, employees, and products and services offered by BALTISEE LIMITED. All business units and locations within TECHNOLOGIES LIMITED, will cooperate to create a cohesive effort in the fight against money laundering.

These procedures are established to guide staff in identifying common practice used in money laundering and terrorism financing, to deter search practice and when discovered or suspected, to use a systematic, uniformed approach for dealing with it. All efforts exerted will be documented and retained. This policy will be applicable for all operations, local and international. The objective of this policy is to ensure that the product and service of BALTISEE LIMITED, are not used to Launder the proceeds of crime and all of the staff is aware of their obligation and the need for vigilance in the fight against money laundering and terrorist finance. The policy of the company is not to enter into business relationships with criminals and terrorists activity and not facilitate any transaction involving criminal or terrorist activity including the finance of terrorism.

The company undertakes to implement all policies and procedures necessary to prevent the money laundering and to comply with all applicable legislations in this regard, such as the regulatory instructions, laws and regulations issued from time to time regulator of the countries where BALTISEE LIMITED, operate. The AML compliance committee is responsible for initiating suspicious activity reports (SARs u)or other required reporting to appropriate law enforcement or regulatory agencies. Any contact by law enforcement and regulatory agency related to the policy shall be directed to the AML compliance committee.

Our AML and CTF program

Our AML and CTF program is made up of the content of this manual. Our activities can be described as a series of controls to manage the way we;

- Accept applications for transactions
- Monitor the transactions we do for unusual activities that need further investigation
- Identify events that require us to take further action
- Report setting matters to our IMoN and;
- Keep a record of what we do

2. GENERAL AND SPECIFIC PROVISION CONCERN MONEY LAUNDERING

Generally, money laundering occurs in three stages. Cash first enters the financial system at the placement stage where the cash generated from criminal activities is converted onto monetary instruments such as money orders or travelers checks, deposited into account at a financial institution. At the integration stage, the funds transferred to move into another account or other financial institution to further separate the money from its criminal origin. At the integration stage the funds uh reintroduce into the economy and used to purchase legitimate assets or to form other criminal activities or legitimate businesses.

Terrorist financing may not involve the proceeds of criminal conduct, but rather I'm an attempt to conceal the origin of intended use of the funds, which will let her be used for criminal purposes. Both individual employees and the company itself are liable for criminal conduct if any of the offenses below are charged by authorities. Money laundering offenses can be distributed as follows:

1. Arrangement relating to criminal property - it is an offense to enter into arrangement 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

2. Tripping off - it is an offense to disclose information which is likely to prejudice and investigate either to the person who is the subject of a money laundering suspicion or any person other than the law enforcement agencies.

3. Acquisition, use of possession of criminal property - it is an offense to acquire, use or possess criminal property

4. Handling the proceeds of corruption- corruption by government leaders and public sectors officials inevitably involves serious crimes. Not only is there a major reputational risk in handling proceed from such activities, but criminal charges and constructive trust suits can arise.

5. Failure to report- it is an offense for a person who knows or suspects or has reasonable grounds for knowing all suspecting that another is engaging In money laundering not to report such knowledge or suspicion as soon as reasonably practical so the authority we are internal reporting procedure.

4. CUSTOMER IDENTIFICATION PROGRAM

BALTISEE TECHNOLOGIES LIMITED has implemented a comprehensive Customer Identification Program (CIP). BALTISEE LIMITED will notify all clients that identification is required and will collect the minimum necessary information from each new customer. All identification documents must come from reputable and verifiable sources.

Information Required from All New Clients

- Full legal name, including any other names used
- Date of birth
- Occupation
- Permanent residential address
- Passport number and country of issuance
- Details of any other government-issued identification evidencing nationality or residence and containing a photograph
- A copy of a government-issued identification document (ID card or passport)
- A valid utility bill in the client's name, not older than three months (e.g., water bill, electricity bill, or bank statement showing the client's name, address, bank name, and account number)

The purpose and intended nature of the business relationship Additional Required Information BALTISEE LIMITED will also record the following for all categories of clients:

Source of wealth (description of the economic/business activity that generated the client's net worth)
Estimated net worth Source of funds to be invested References or supporting documentation to validate the client's reputation, where available Corporate Customers For companies listed on a recognized or approved stock exchange—or companies wholly owned by such entities—no additional identity verification is required beyond standard commercial due-diligence checks.

For unlisted companies,
BALTISEE LIMITED will conduct a full identification and verification process to confirm the company's legal existence, good standing, and the authority of individuals acting on its behalf. Required documentation may vary by jurisdiction but typically includes:

- Certificate of Incorporation or equivalent document confirming the company's legal registration and registered address

- Shareholder register (if not included in the Certificate of Incorporation)
- Certificate of Incumbency or equivalent document listing current directors
- Memorandum and Articles of Association or equivalent documents confirming officer authority
- Extract from the official commercial register, where applicable

Verifying Information
BALTISEE LIMITED will take all reasonable and practicable steps to ensure that the true identity of each customer is verified, based on the assessed risk level.

Verification procedures include: Review of valid photo identification Reliance on government-issued documents to confirm identity.
All documents must be obtained as originals or certified copies. Acceptable certifying authorities include:

- A notary public or other legally authorized certifier
- A state official (e.g., judge, police officer, consular official)
- An authorized financial institution
- Official online registries, provided a BALTISEE staff member prints and stores the document in the client's file
- The Money Laundering Reporting Officer (MLRO) is responsible for verifying customer identities and ensuring that all verification steps are completed before a customer agreement is issued, except in exceptional circumstances approved by the Compliance Officer.

The MLRO will additionally check all clients against sanctions and compliance lists using the automated search system SUM & SUM.

Any individual or entity appearing on a sanctions list will not be on boarded by BALTISEE TECHNOLOGIES LIMITED.

HIGH-RISK CATEGORIES

High-Risk Countries

Clients or beneficial owners residing in, or whose funds originate from, countries identified as having inadequate anti-money-laundering controls or high levels of corruption will be subject to enhanced due diligence.

Offshore Jurisdictions

Although standard due-diligence procedures apply, BALTISEE LIMITED will implement stricter controls for clients or beneficial owners linked to offshore jurisdictions.

High-Risk Activities

Clients whose wealth derives from activities known to be vulnerable to money laundering will undergo heightened scrutiny.

Public Officials (PEPs)

Individuals holding or formerly holding prominent public positions—including government officials, senior executives of state-owned enterprises, politicians, and political party officials—along with their families and close associates, will be subject to enhanced scrutiny.

5. COMPLIANCE OFFICER

1. Money laundering compliance officer

Name : Robert Briggs

Email address: support@via.top

1. Roles and responsibilities

The compliance officer will be responsible for:

1. Creating and keeping this manual current:
2. Monitoring the compliance by our business with the requirement of the laws and regulation that related to AML and CTA
3. Monitoring transactions undertaking for customers
4. Identification and management of money laundering risk using our service
5. Providing leadership and training on AML & CTF issues to our staff, including new Staff
6. Acting as a liaison point with the IMoLIN
7. Investigating unusual matters and reporting those that are suspicious to our IMoLIN
8. Reporting all other matters that must be reporting to the IMoLIN
9. Ensuring our staff knows what their responsibilities are
10. Monitoring employees in the course of performance of their duties
11. Ensuring that our staff are aware of the requirement of this manual and of the AML and CTF laws and regulations that applied to our business.
12. Reviewing this manual periodically for its adequacy

6. STAFF TRAINING AND AWARENESS

It is essential that everyone in the company understands what they have to do to comply with the requirement of the manual All staff are expected to comply fully with all the procedures of this manual and are expected to report any unusual or suspicious activity detected to the compliance officer.

Staff dealing with day-to-day transactions, are encouraged to consult with the compliance officer through the feel that a transaction could be considered suspicious for whatever reasons or that a client is behaving or dealing with the company in a suspicious manner.

All Staff are expected to understand the law regarding tipping off and comply with our anti tipping off procedure All staff are expected to cooperate with the compliance officer and the IMoLIN pending investigation of any possible breaches of the laws that are related to the AML & CTF.

7. MONITORING AND REPORTING

We are required to maintain business records in order to meet the legal obligations of the Republic of Ireland and to ensure that all transactions can be readily reconstructed at any time.

All applications and documents used to verify identity must be retained for six years following the closure or termination of the account, service, or business relationship.

Transaction-based monitoring will be carried out within the relevant business units of TECHNOLOGIES LIMITED. Monitoring of specific transactions will include, but is not limited to, transactions totaling USD 5,000 or more, as well as any transactions that TECHNOLOGIES LIMITED has reason to suspect involve suspicious activity. All reports will be fully documented.

If a transaction exceeds the established parameters, and the client's explanation is unsatisfactory or gives rise to suspicion, staff are required to consult with the Director responsible for that client to document and file a Suspicious Transaction Report.

All reports submitted to the IMoLIN must have the written authorization of the Director and must be discussed with the Company's Compliance Officer.

Staff are reminded that a Suspicious Transaction Report filed with TECHNOLOGIES LIMITED must not be disclosed to the client or to any parties involved in the reported transaction. Such reports must remain strictly confidential between the Company and IMoLIN

8. SUSPICIOUS ACTIVITY

The customer shows unusual concern about the Company's compliance with government reporting requirements or AML policies, particularly regarding their identity, business type, or assets, or is reluctant/refuses to provide information about their business activities. The customer may also present unusual or suspicious identification or business documents.

The customer attempts to engage in transactions that lack business rationale or a clear investment strategy, or that are inconsistent with their stated business operations.

Information provided by the customer to establish a legitimate source of funds is false, misleading, or substantially incorrect.

The customer refuses or fails to identify any legitimate source for their funds or assets when requested.

The customer has a questionable background or is mentioned in media reports suggesting potential criminal, civil, or regulatory violations.

The customer displays a lack of concern for risks, commissions, or transaction costs.

The customer appears to act on behalf of an undisclosed principal but is unwilling or hesitant—without legitimate commercial reasons—to provide information about the person or entity represented.

The customer cannot clearly describe the nature of their business or demonstrates limited knowledge of their own industry.

The customer engages in cash or cash-equivalent transactions structured to avoid government reporting requirements, especially when amounts fall just below reporting thresholds.

The customer's account shows sudden, unexplained wire transfer activity, particularly when the account previously had little or no activity.

The customer conducts a large number of wire transfers to unrelated third parties that do not align with their legitimate business purpose.

The customer deposits funds and immediately requests that the money be wired or transferred to a third party or another firm without any apparent business justification.

The customer performs excessive journal entries between unrelated accounts without a clear business purpose.

The customer's account reflects unusually high activity levels coupled with very low volumes of securities transactions.

9. INVESTIGATION

Upon notification to the AML Compliance Committee, an investigation will be initiated to determine whether a report should be filed with the appropriate law enforcement or regulatory agencies. The investigation will include but is not limited to—a review of all available information, such as payment history, birth dates, and addresses. If the results of the investigation warrant, a recommendation will be made to the AML Compliance Committee to file a blocked assets report and/or a Suspicious Activity Report (SAR) with the relevant authorities.

The AML Compliance Committee is responsible for issuing any notices or filings to law enforcement or regulatory agencies.

The results of an investigation must not be disclosed or discussed with anyone except those who have a legitimate need to know. Under no circumstances shall any officer, employee, or appointed agent disclose or discuss any AML concern, investigation, notice, or SAR filing with the individual(s) who are the subject of such matters, nor with any other person, including members of the officer's, employee's, or agent's family.

Maintaining confidentiality during an investigation is of critical importance. Employees are reminded of the offence of “tipping off.” TECHNOLOGIES LIMITED reserves the right to immediately terminate its agreement with a client and to prohibit the client from withdrawing any assets if the explanations provided are inadequate or inconsistent with the AML Policy.

10. INTERNAL AUDIT

The AML Compliance Committee and the audit functions are segregated to ensure that the activities of the compliance function are subject to independent review. The Compliance Officer will periodically arrange for this manual to be reviewed by an independent party to assess its adequacy and compliance.

The audit function should, of course, keep the Compliance Officer informed of any audit findings that relate to compliance. However, the Compliance Officer—and any member of their staff—may not conduct this independent review.

The report from the independent review will be provided to the owner and the Compliance Officer. The Compliance Officer will implement any required remediation actions identified in the report, provided they are practical and appropriate