4XHUB INTERNATIONAL LTD

AML/CFT POLICY

TABLE OF CONTENTS

GLOSSARY OF TERMS

AML/CFT	Anti-Money Laundering and Combating the Financing of Terrorism and Proliferation
CDD	Client Due Diligence
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FIAMLA	Financial Intelligence and Anti-Money Laundering Act 2002
FIAMLR	Financial Intelligence and Anti Money Laundering Regulations 2018
FIU	Financial Intelligence Unit
FSC	Financial Services Commission of Mauritius
FSC Handbook	Anti-Money Laundering and Countering the Financing of Terrorism Handbook
KYC	Know Your Client
MLRO	Money Laundering Reporting Officer
NCCT	Non-Cooperative Countries and Territories
PEP	Politically Exposed Person
ROC	Registrar of Companies

SECTION I

GENERAL

CODE FOR GENERAL RULES OF CONDUCT AND CODE OF ETHICS

This Internal Control Manual sets forth ethical principles and standards of conduct to be complied with by all employees of 4XHUB INTERNATIONAL LTD (the “Company”)

All officers and employees are expected to follow certain patterns of good conduct that have long prevailed in the financial services sector. This Manual does not substitute these principles, laws, Handbook or other code of conduct issued by the FSC and any other applicable regulators, but only complements and enhances them.

The Company encourages at all times high standards of business and personal conduct. This Manual brings together the relevant internal procedures set up by the Company in order to be compliant with its policies, with the law and licence conditions.

Specifically, it addresses the rules and regulations of the FSC which is the regulator for all non-bank financial services in Mauritius, and encompasses the procedures in place to ensure compliance with local laws, including, without limitation to, the Financial Services Act 2007, the Securities Act 2005 and the regulations made thereunder, the Financial Intelligence and Anti-Money Laundering Act 2002, the Financial Intelligence and Anti-Money Laundering Regulations 2018 and the United Nations (Financial Restrictions, Arms Embargo and Travel Ban) Act 2019.

Good compliance is good business, and is also vital to sustain in business. Any company that does not believe in this principle will not remain in business. The preservation of the good name and reputation built along time requires the adoption of policies to prevent situations in which there may be conflicts of interest among clients, the Company and/or its employees. The Company by the very nature of its business deals with confidential privileged information; and hence there is a greater possibility that conflict of interest may occur.

Therefore, all officers and employees are expected to have read and understood the contents of this Manual in so far as it is applicable to him/her and shall abide by these principles and any deviation from them will not be tolerated. The Company’s staff must also refer and keep themselves up to date

with the relevant rules and regulations applicable to the Company and which is generally available at the regulator's website www.fscmauritius.org.

The Company may bring changes to this Manual from time to time to reflect changes in its business policies, international best practices and regulatory or legislative changes.

This Manual does not seek to encompass all the relevant laws applicable to the Company. Employees are encouraged to always refer to the applicable laws.

GENERAL RULES OF CONDUCT

In order to fulfil this role, the Company needs to maintain the confidence of its clients, shareholders and employees, and other stakeholders by acting with professionalism and integrity as well as behaving with prudence and skill.

The Company, therefore, attaches paramount importance to upholding its reputation. It is the responsibility of everyone in the Company to maintain its standing for high ethical standards of conduct. This requires constant vigilance and application.

The General rules described in this statement do not merely reflect laws and regulations; they are also based upon values of integrity, entrepreneurship, professionalism, responsiveness and teamwork.

These General rules apply to the whole of the Company and all employees who are required to act in accordance with both the letter and spirit of these General rules. It is the responsibility of all those in authority in the Company to ensure that these General rules are fully communicated to all employees and that they are strictly observed.

All staff members are required to comply with all applicable laws, rules and regulations, whether or not specifically addressed in this Manual. Whenever a difficulty arises over the application or meaning of a particular rule or regulation, recourse should always be made to the compliance officer of the Company (the "Compliance Officer") whose functions are more fully particularised below.

If required, FSC's officers should be given access to examine and question the Company and individual staff members on its records, IT systems, office procedures and its manual. Staff must co-

operate fully with any FSC supervision team visiting the Company, including, but not limited to, answering all questions posed by the inspectors, truthfully and without constraint. Any staff member receiving a request for assistance, evidence or any other information from outside regulatory bodies should immediately enlist the assistance of the Compliance Officer.

Staff members should not make direct contact with the FSC but should address questions or concerns about any compliance or regulatory issue to the nominated Compliance Officer.

COMPLIANCE OFFICER

The Compliance Officer, who shall be a natural person and approved by the FSC, is the officer primarily responsible for overseeing and managing compliance issues within the Company. He/She has a duty to report to the Board or any other person appointed by the Board on the progress of implementation and review of the Company's policies and procedures and staff training. In the event of the Compliance Officer's absence from the Company, one of the directors of the Company will act as the alternate compliance officer and will assume the responsibilities of the Compliance Officer.

The main responsibilities of the Compliance Officer are:

- The effective implementation of the provisions contained in this Manual;
- The effective implementation of the applicable laws and regulations;
- Brief the directors of the Company on matters relating to compliance;
- Ensure that the staff of the Company are trained on a regular and continuous basis to ensure that they understand this Manual and the laws relating to Anti Money Laundering and Prevention of Corruption;
- Advise directors on the impact of likely changes in legislation and procedures relating to compliance matters;
- Meet the external notification and the reporting requirements relating to statutory, regulatory and supervisory matters;
- Conduct review of files to generally ensure that all compliance requirements are met;
- Determine whether any existing business relationships exist with persons or groups with known or suspected links to terrorist activity
- Conduct similar reviews when names are added to any existing lists of known or suspected terrorists;

- On a pro-active basis, identify and assess the compliance risks associated with the company activities, including in relation to the development of new products and business practices, the proposed establishment of new business or customer relationships, or material changes in the nature of such relationships;
- Establish written guidance to staff on the appropriate implementation of the laws, rules and standards through policies and procedures and, when necessary, formulating proposals for amendments;
- Monitor compliance with policy by performing regular and comprehensive compliance risk assessment and testing, and reporting on a regular basis to Senior Management, and if necessary, the Board or a committee of the Board, on compliance matters, the reports should refer to the compliance risk assessment and testing which has taken place during the reporting period, any identified breaches and/or deficiencies, and the corrective action taken; the reports should also contain information about compliance function and other staff;
- Educate staff with respect to compliance with the applicable laws, rules and standards, and acting as a contact point within the Company and other staff;
- Liaise with relevant external bodies, including regulators, and external legal counsel.

The Compliance Officer shall also ensure to:

- Analyse regularly the business and compliance risks;
- Review the compliance strategy;
- Reassess the compliance standards in place and analyse how current standards are being met;
- Review training and competence arrangements;
- Broaden and deepen relationships with the regulator;
- Review Senior Management responsibilities;
- Review the structure and reporting lines of the Compliance Department;
- Consider the adequacy of compliance resources;
- Assess how well compliance issues are being communicated and acted upon;
- Build compliance into the Company's Day to day management decision processes;
- Build compliance into the governance of the Company.
- Perform compliance monitoring subject to an approved plan
- Perform compliance risk management subject to an approved yearly plan which is reportable every quarter.

- Provide regular communication and training to all staff on matters arising from the monitoring and risk management plans.

OPERATING PRINCIPLES

PERSONAL CONDUCT

The Company expects the highest levels of personal conduct by all its employees, whatever their position. It is acknowledged that all effective business relationships depend upon honesty, integrity and fairness.

While it is recognized that limited corporate hospitality is given and received as part of building normal business relationships, employees should avoid accepting hospitality or gifts that might appear to place them under an obligation.

Bribery of any form is unacceptable. No undeclared offers or payments will be accepted or solicited by employees, or made by employees to third parties, and employees are required to avoid any contacts that might lead to, or suggest, a conflict of interest between their personal activities and the business of the Company.

The Company expects all its employees to respect the rule of law and abide by appropriate regulations. Furthermore, all employees are expected to avoid doing business with any individual, company or institution if that business is connected with activities which are illegal or which could be regarded as unethical.

When an employee is recruited and/or accedes to a Senior Officer role, the employee shall provide to the Company a Certificate of Character dated not more than 1 month from the date of appointment.

DEALING WITH AUDITORS AND LEGAL COUNSEL

The Company will respond honestly and candidly and disclose information fully, accurately when dealing with the Company's independent and internal auditors, regulators and attorneys.

OPERATION

The Company wishes to have an unimpeachable reputation for integrity; therefore, it is essential that the Company can be judged by its actions. As these business principles make clear, this depends upon the conduct of every individual in the Company.

All employees must be familiar with these standards and apply them consistently and rigorously in business activities each day. It is important that the conduct of a few, whether through misplaced zeal or short-term expediency, should not damage the reputation of the many in the Company.

All employees are responsible for the application of the principles across the Company, and must lead by example.

The most effective assurance mechanism is constant vigilance by all of employees, at all times, to ensure that the Company is clearly seen to act in keeping with the commitment to maintain high ethical standards.

FAIR DEALING

The Company will seek competitive advantage through superior and honest performance, never through unethical or illegal business practices. It will endeavor to deal fairly and honestly with:

- Company's Clients
- Suppliers
- Competitors
- Vendors

The Company will not take unfair advantage of anyone through manipulation, concealment, abuse of privileged information, misrepresentation of material facts or any unfair dealing.

BUSINESS RISK ASSESSMENT

Pursuant to Section 17(1) of the FIAMLA, a financial institution must identify, assess, understand and monitor money laundering and terrorism financing risks.

While performing business, Management, Compliance and Risk Management should all work together on performing the Business Risk Assessment. Primarily, responsibility for the quality and execution of the risk analyses lies with the first line of defence. This is the business, as risks manifest themselves first there. The role of Compliance is process monitoring, facilitating and testing. Other functions or departments such as Audit can also provide the necessary input. The ultimate responsibility for the Business Risk Assessment lies with the board of directors.

The 6 key areas which will be assessed when undertaking the business risk assessment amongst other risk factors are:

i. the nature, scale and complexity of the financial institution's activities;
ii. the products and services provided by the financial institution's;
iii. the persons to whom and the manner in which the products and services are provided;
iv. the nature, scale, complexity and location of the customer's activities;
v. reliance on third parties for elements of the customer due diligence process; and
vi. technological developments.

The Business Risk Assessment and any review thereof shall take into account the findings of the National Risk Assessment and any guidance issued.

Furthermore, the Company undertakes to update the Business Risk Assessment on an annual basis or at shorter intervals in case of need.

SECTION II

AML/CFT MANUAL

INTRODUCTION

The commitment of 4XHUB INTERNATIONAL LTD to prevent the wrongful use of its services has led to the implementation of policies, the creation of an effective compliance culture and the drafting of this comprehensive Manual.

It emphasizes several procedures to follow and is in line with applicable laws, regulations and guidelines.

4XHUB INTERNATIONAL LTD strongly believes in an effective internal compliance culture and encourages all of its staff members to be vigilant and sensitive to any apparent wrong-doing.

Even in cases of referred clients, 4XHUB INTERNATIONAL LTD *will not rely on the KYC provided by the introducers to accept those clients.*

It is the responsibility of the Board to manage the Company effectively and ensure compliance with applicable laws and regulations. From an AML/CFT perspective, the Board needs to:

(a) have broad oversight on compliance with the provisions of this Policy and providing guidelines regarding the management of AML/CFT compliance risks on a risk based approach;

(b) ensure that systems and controls are appropriately designed, documented and implemented, and are effectively operated to reduce the risk of the business being used in connection with AML/CFT;

(c) ensure that the AML/CFT framework devised for the Company is reviewed and kept relevant and up to date;

(d) determine the nature and extent of compliance reviews commensurate with the risk assessments, size and nature of business of the Company;

(e) appoint all relevant officers required under the relevant AML/CFT regulations including a compliance officer, a money laundering reporting officer (MLRO) and a deputy money laundering reporting officer (DMLRO) and apportion responsibilities for combatting AML/CFT;

(f) be responsible for reviewing and making decisions, based on reports received on AML/CFT matters;

(g) devise screening procedures to ensure high standards when hiring employees;

(h) implement an ongoing training programme for its directors, officers and employees, as applicable, to maintain awareness of the Relevant Laws;

(i) maintain records in line with the regulatory requirements, and

(j) appoint an independent audit function to test the policies, procedures and controls of the Company regarding AML/CFT.

In line with its overarching responsibility for AML/CFT, the Board needs to proceed in accordance with the Relevant Laws, with the appointment of key persons within the Company. These include but are not limited to the Compliance Officer, the Money Laundering Reporting Officer and the Deputy Money Laundering Officer.

KEY DEFINITIONS

WHAT IS MONEY LAUNDERING?

Money Laundering is a process through which illegally gained proceeds are brought back into the economy as legitimate income.

The Financial Action Task Force describes Money Laundering as “the processing of criminal proceeds in order to disguise their illegal origin”.

Examples of crimes through which dirty money may be obtained include kidnapping, drug trafficking, bribery/corruption, forgery, prostitution, smuggling, extortion, and tax evasion.

OBJECTIVES OF MONEY LAUNDERING

- To conceal the origin and true ownership of criminal proceeds

- To maintain control over the proceeds
- To enjoy profits of crime in the guise of legitimate business

There are three recognised forms of the Money Laundering process:

PLACEMENT

This is the stage at which illicit funds are separated from their illegal source. Placement involves the initial injection of the illegal funds into the financial system or carrying of cash across borders.

LAYERING

This is the stage at which the launderer engages in a series of conversions or movements of the funds to distance them from their source. Money laundering requires the creation of multiple layers of transactions that further separate the funds from their illegal source. The purpose of this stage is to make it more difficult to trace these funds to their illegal source.

INTEGRATION

This is the stage at which the funds re-enter the legitimate economy. The funds now appear as clean income.

WHAT IS TERRORIST FINANCING?

Terrorist financing is the provision or collection of funds by any means, directly or indirectly, with the intention that they should be used, in full or in part, in order to carry out terrorist offences.

Acts of terror and the terrorist groups that commit them require funding in much the same way that criminal organisations require money to further their criminal activities.

WHAT IS PROLIFERATION FINANCING?

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

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

DEFINITIONS UNDER THE FIAML REGULATIONS 2018

1. "Applicant for business" means a person, who seeks to form a business relationship, or carry out an occasional with a reporting person.

2. "customer" means a natural person or a legal person or a legal arrangement for whom a transaction or account is arranged, opened or undertaken and includes —

    (a) a signatory to a transaction or account;

    (b) any person to whom an account or rights or obligations under a transaction have been assigned or transferred;

    (c) any person who is authorised to conduct a transaction or control an account;

    (d) any person who attempts to take any action referred to above;

    (e) an applicant for business;

DEFINITIONS UNDER THE FIAMLA 2002

1. "financial institution" means –

    (a) an institution or a person, as the case may be, licensed, registered or authorised under –

        (i) section 14, 77, 77A or 79A of the Financial Services Act;

        (ii) the Insurance Act, other than an insurance salesperson;

        (iii) the Securities Act; (iv) the Captive Insurance Act; or

(v) the Trusts Act; or

(b) a credit union;

2. "suspicious transaction" means a transaction which –

(a) gives rise to a reasonable suspicion that it may involve–

(i) the laundering of money or the proceeds of any crime; or

(ii) funds linked or related to, or to be used for, the financing of terrorism or proliferation financing or, any other activities or transaction related to terrorism as specified in the Prevention of Terrorism Act or under any other enactment, whether or not the funds represent the proceeds of a crime;

(b) is made in circumstances of unusual or unjustified complexity;

(c) appears to have no economic justification or lawful objective;

(d) is made by or on behalf of a person whose identity has not been established to the satisfaction of the person with whom the transaction is made; or

(e) gives rise to suspicion for any other reason.

The following are some indicators of potentially suspicious activity, and should arouse scepticism as the source of funds for the transaction:

- Any activity that casts doubt over the true identity of an applicant for business or principals thereof;
- Establishment of companies having no obvious commercial purpose;
- Unusually linked transactions;
- Unwillingness to disclose source of funds;
- Complex structures with no obvious commercial purpose;
- Activities that appear to be inconsistent with the KYC information and profile of the Client;
- Fund transfer to or from accounts in Financial Action Task Force (“FATF”) non co-operative countries and territories or countries that are known to be associated with drug trafficking or other serious crimes.

The FIU, established under the FIAMLA, is the central agency in Mauritius responsible for receiving, requesting, analyzing and disseminating to the investigatory and supervisory authorities, disclosures of financial information.

PREVENTION OF MONEY LAUNDERING, TERRORIST AND PROLIFERATION FINANCING

. In particular, the Board shall ensure that at all times:

- There is appointed a Compliance Officer, a Money Laundering Reporting Officer ("MLRO") and a Deputy MLRO in accordance with the Handbook, and such persons shall be part of Senior Management;

- The Company has appropriate access to an international database to conduct verification of identity of parties that the Company may deal with;

- The Company will not accept client relationships which are reasonably believed to be involved or tainted with money-laundering, terrorist or proliferation financing practices;

- The "Know Your Client" ("KYC") principle is central and as such, one of the most important weapons guarding against money launderers. It is imperative that any member of staff dealing with a client must:

    - know the client, including the beneficial owner(s) and ultimate beneficial owneras well as understand the nature of transaction to be expected from him and the source of the funds involved;
    - proceed to all verifications and identification as well as keeping records, registers or document required under the applicable laws;

- The member of staff has to be aware that he/she has a duty to report any suspicious transaction to the MLRO and that if he/she fails to do so then the liability might lie with him/her. In all circumstances, the MLRO should be apprised of the situation with the least possible delay.

- The report should be internal and concise, accompanied by all documentation that gives rise to the suspicion. In the event of the transaction not being reported, the reason for not doing so must still be recorded for future reference. Furthermore, in the event that any mitigating factor by way of trustworthy information or document(s) which clears the initial suspicion

about the transaction is obtained after sending the internal report, such information or document(s) should immediately be sent to the MLRO together with an additional report.

- Members of staff will have to undergo regular training programs which explain all applicable anti-money laundering laws and regulations and recent trends in money laundering.

SUSPICIOUS TRANSACTIONS

WHY DO WE HAVE SUSPICIOUS TRANSACTION PROCEDURES?

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

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

It is the duty of the employee under the law to make a report of any suspicious transaction that he/she comes across and where an employee makes a suspicious transaction report to the MLRO, he/she will have discharged his/her legal obligation to report under the Financial Intelligence and Anti-Money Laundering Act 2002.

The STR should be remitted directly to the MLRO or the Alternate MLRO and not be compromised by any other member of staff within the Company. As soon as the MLRO receives the report, all details will be logged. The MLRO shall acknowledge the internal STR.

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

If the investigation can unequivocally be found to be without foundation and not suspicious, then the matter is closed and the findings logged.

If there is any reasonable suspicion, then a full report must be submitted to the FIU and the relevant details entered into the STR log. Accordingly, the client will be classified and treated as high-risk.

The MLRO will also inform senior management that the clients should be treated as high risk and the risk rating changed accordingly.

NOTE

Tipping Off is considered as a very serious offence by the local regulator. It is the deliberate act of informing the party under suspicion that they are being investigated.

'Tipping off' the client or any other person is a criminal offence under Section 16
of the FIAMLA 2002 and upon conviction, the penalty is a fine not exceeding 5 million rupees and imprisonment not exceeding 10 years.

Malicious reporting: If anyone submits an STR to the FIU without reasonable grounds or maliciously, the Company may be sued for breach of client confidentiality.
However, if a disclosure is made in good faith but proves to be groundless, then the Company may claim immunity.

DUTIES UNDER FIAMLA AND FIAML REGULATIONS 2018

Section 14(1) of the FIAMLA states that:

Notwithstanding section 300 of the Criminal Code and any other enactment, every reporting person or auditor shall, as soon as he becomes aware of a suspicious transaction, make a report to FIU of such transaction not later than 5 working days after the suspicion arose.

Section 17(1) of the FIAMLA states that:

Risk assessment

(1) Every reporting person shall –

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

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

Section 17C(b)(i) of the FIAMLA states that:

17C. Customer due diligence requirements

(1) A reporting person shall undertake CDD measures as may be prescribed, and in the following circumstances –

(b) where a customer who is neither an account holder nor in an established business relationship with the reporting person wishes to carry out –

(i) a transaction in an amount equal to or above 500, 000 rupees or an equivalent amount in foreign currency or such amount as may be prescribed, whether conducted as a single transaction or several transactions that appear to be linked; or

Regulation 4(1), (2) of the FIAML Regulations 2018 states that:

(1) For a customer who is a natural person, a reporting person shall obtain and verify-

(a) the full legal and any other names, including, marital name, former legal name or alias;
(b) the date and place of birth;
(c) the nationality;
(d) the current and permanent address; and
(e) such other information as may be specified by a relevant supervisory authority or regulatory body.

(2) For the purposes of paragraph (1), documentary evidence as may be specified by a relevant regulatory body or supervisory authority shall be used for the purposes of verification of identity requirement.

Regulation 9(1) of the FIAML Regulations 2018 states that:

"(……) a reporting person shall verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers."

Regulation 26(1) and (4) of the FIAML Regulations 2018 states that:

26. (1) A reporting person shall appoint a Money Laundering Reporting Officer to whom an internal report shall be made of any information or other matter which comes to the attention of any person handling a transaction and which, in the opinion of the person gives rise to knowledge or reasonable suspicion that another person is engaged in money laundering or the financing of terrorism.

(4) The Money Laundering Reporting Officer and the Deputy Money Laundering Officer shall —

(a) be sufficiently senior in the organisation of the reporting person or have sufficient experience and authority; and

(b) have a right of direct access to the board of directors of the reporting person and have sufficient time and resources to effectively discharge his functions.

Regulation 17F(2) of the FIAMLA 2002 states that:

(2) The books and records maintained by the reporting person for all the customers and transactions shall include –

(a) all records obtained through CDD measures, including account files, business correspondence and copies of all documents evidencing the identity of customers and beneficial owners, and records and the results of any analysis undertaken in accordance with this Act, all of which shall be maintained for a period of not less than 7 years after the business relationship has ended;

(b) records on transactions, that are sufficient to permit reconstruction of each individual transaction, which shall be maintained for a period of 7 years after the completion of the transaction; and

(c) copies of all suspicious transaction reports made pursuant to section 14 or other reports made to FIU in accordance with this Act, including any accompanying documentation, which shall be maintained for a period of at least 7 years from the date the report was made.

Regulation 25(1) of the FIAML Regulations 2018 states that:

25. (1) A reporting person shall examine, as far as reasonably possible, the background and purpose of all transactions that — (a) are complex transactions; (b) are unusually large transactions: (c) are conducted in an unusual pattern; or (d) do not have an apparent economic or lawful purpose. (2) Where the risks of money laundering or terrorism financing are higher, a reporting person shall conduct enhanced CDD measures consistent with the risk identified.

IDENTIFYING A SUSPICIOUS TRANSACTION

Refer to the Guidance Note 3 issued by the Financial Intelligence Unit (FIU), in force with effect from 21 January 2014, and Paragraphs 10.3 and 10.5 of the Handbook, for information *inter alia* on how to identify a Suspicious Transaction.

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

Refer to Annexure I of this AML/CFT Manual for a list of indicators of potentially suspicious activity. This list is, however, not an exhaustive list.

INTERNAL PROCEDURE FOR THE REPORTING OF SUSPICIOUS TRANSACTIONS

Staff must report any suspicious transaction to the Money Laundering Reporting Officer (MLRO) using the Internal Disclosure Form, in order to discharge their reporting legal obligations.

The MLRO of 4XHUB INTERNATIONAL LTD will review the matter and evaluate the Internal Disclosure, after which a report to the Financial Intelligence Unit (FIU) will be made – as and when required within 5 days.

In the absence of the MLRO, any Suspicious Transaction should be reported to the Deputy MLRO of 4XHUB INTERNATIONAL LTD on the Internal Disclosure Form.

.

The MLRO shall be a natural person of sufficiently senior status or who has sufficient experience and authority. Prior approval of the FSC shall be sought for the appointment of the MLRO. The MLRO should have a right of direct access to the board of directors of the Company and has sufficient time and resources to effectively discharge his/her functions effectively and autonomously.

The MLRO is the person to whom an internal report should be made of any information or other matter which comes to the attention of any person handling a transaction and which, in the opinion of that person gives rise to knowledge or reasonable suspicion that another person(s) is engaged in AML/CFT. The MLRO shall consider and assess such internal reports to determine whether an external disclosure to the relevant local authority is required. A DMLRO should also be appointed in order to exercise the functions in the MLRO's absence. The DMLRO should be of similar status and experience as the MLRO. The MLRO/DMLRO shall treat all internal disclosures with utmost confidentiality.

In the discharge of his functions, the MLRO acts with total autonomy and independence and shall be the main point of contact of the Company with the FIU.

The Company needs to ensure that the MLRO and DMLRO have unfettered access to CDD information on customers and beneficial owners thereof.

The Company needs to further ensure that the identity and contact details of the MLRO are disclosed to all relevant staff and that he/she should be contactable on a day to day basis.

The MLRO shall receive in depth and ongoing training on all aspects of AML/CFT. As currently prescribed by the Competency Standards, the MLRO and DMLRO need to complete a minimum of 10 CPD hours of AML/CFT training.

The responsibilities of the MLRO includes:

(a) undertaking a review of all internal disclosures in the light of all available relevant information and determining whether or not such internal disclosures warrant an external disclosure to be made to the FIU;

(b) fully document the internal disclosure evaluation process;

(c) maintaining the STR log and all related records;

(d) assist relevant staff with guidance on disclosures and tipping off if any disclosure is made;

(e) liaising with and be the main point of contact with the FIU and if required the FSC and participating in any other third-party enquiries in relation to money laundering or terrorist financing prevention, detection, investigation or compliance;

(f) register on the GOAML platform for STR reporting; and

The MLRO shall have direct access to the Board and provide reports and other information to senior management and/or the board of directors at such frequency as determined by the Board.

DUE DILIGENCE

4XHUB INTERNATIONAL LTD must undertake CDD measures and be satisfied of the results obtained:

Section 17F of the FIAMLA:

(1) "A reporting person shall maintain all books and records with respect to his customers and transactions and shall ensure that such records and books are kept for such time as specified in, and in accordance with, the Act.

All transactional records must be retained for the duration of the client relationship and for a period of at least seven years after the completion of the transaction to which it relates.

Identity records should be maintained for the duration of each relationship and for a period of at least 7 years thereafter.

Records of all anti-money laundering training delivered to employees must also be maintained.

Records of internal Suspicious Transaction Reports (STRs) made and STRs filed with the FIU should be maintained for the duration of the client relationship and all records should be retained for a period of at least 7 years after the completion of the transaction.

Regulation 4(1), (2) of the FIAML Regulations 2018 states that:

4. (1) For a customer who is a natural person, a reporting person shall obtain and verify —

(a) the full legal and any other names, including, marital name, former legal name or alias;

(b) the date and place of birth;

(c) the nationality;

(d) the current and permanent address; and

(e) such other information as may be specified by a relevant supervisory authority or regulatory body.

(2) For the purposes of paragraph (1), documentary evidence as may be specified by a relevant regulatory body or supervisory authority shall be used for the purposes of verification of identity requirement.

Regulation 9(1) of the FIAML Regulations2018states that:

"(……) a reporting person shall verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers."

Procedures to be followed in regards to the above;

a. Obtain confirmation on source of funds

b. Assess the applicant's business activity

c. Ask for further clarifications if the source of funds and the business activity do not tally

d. If the applicant agrees that he is acting on behalf of a third party, request the following:

i. where the third party is a natural person, the identity of that third party;

ii. where the third party is a body corporate or unincorporated, proof of identity such as

a. Official documents and such other information as may be required which collectively establish their legal existence

b. A certified copy of the resolution of the Board of Directors or managing body and the power of attorney granted to its managers, officers or employees to transact on its behalf

iii. the relationship between the third party and the applicant for business.

In case it has not been determined whether the applicant for business is acting for a third party, the procedure should be as follows:

i. make a record of the grounds for suspecting that the applicant for business is so acting; and

ii. make a suspicious transaction report to the Financial Intelligence Unit"

Regulation 26(1) and (4) of the FIAML Regulations 2018 states that:

26. (1) A reporting person shall appoint a Money Laundering Reporting Officer to whom an internal report shall be made of any information or other matter which comes to the attention of any person handling a transaction and which, in the opinion of the person gives rise to knowledge or reasonable suspicion that another person is engaged in money laundering or the financing of terrorism.

(4) The Money Laundering Reporting Officer and the Deputy Money Laundering Officer shall —

(a) be sufficiently senior in the organisation of the reporting person or have sufficient experience and authority; and

(b) have a right of direct access to the board of directors of the reporting person and have sufficient time and resources to effectively discharge his functions.

Regulation 17F(2) of the FIAML Regulations 2018 states that:

(2) The books and records maintained by the reporting person for all the customers and transactions shall include –

(a) all records obtained through CDD measures, including account files, business correspondence and copies of all documents evidencing the identity of customers and beneficial owners, and records and the results of any analysis undertaken in accordance with this Act, all of which shall be maintained for a period of not less than 7 years after the business relationship has ended;

(b) records on transactions, both domestic and international, that are sufficient to permit reconstruction of each individual transaction for both account holders and non-account holders, which shall be maintained for a period of 7 years after the completion of the transaction; and

(c) copies of all suspicious transaction reports made pursuant to section 14 or other reports made to FIU in accordance with this Act, including any accompanying documentation, which shall be maintained for a period of at least 7 years from the date the report was made.

Regulation25(1) of the FIAML Regulations 2018 states that:

25. (1) A reporting person shall examine, as far as reasonably possible, the background and purpose of all transactions that — (a) are complex transactions; (b) are unusually large transactions: (c) are conducted in an unusual pattern; or (d) do not have an apparent economic or lawful purpose. (2) Where the risks of money laundering or terrorism financing are higher, a reporting person shall conduct enhanced CDD measures consistent with the risk identified.

AML/CFT INDEPENDENT AUDIT

Scope of Independent Audit

By virtue of the FIAMLA and FIAML Regulations 2018, there is a statutory obligation on every financial institution to have in place an independent audit function which will allow the reporting entity to evaluate its AML/CFT programme and to ascertain whether the established policies, procedures, systems and controls are adapted with the money laundering and terrorism financing risks identified. The objective of an independent AML/CFT audit is to form a view of the overall integrity and effectiveness of the AML programme, including policies, procedures and processes.

Further guidance with respect to the independent AML/CFT audit is provided at Chapter 13 of the Handbook.

The Company undertakes to conduct an independent AML/CFT audit on an annual basis. The following non- exhaustive areas shall be tested:

- AML/CFT policies and procedures;
- Internal Risk Assessment;
- Risk Assessment on the use of third-party service providers (Outsourcing);
- Compliance Officer function and effectiveness;
- MLRO function and effectiveness;
- Implementation and Effectiveness of Mitigating Controls, including customer due diligence and enhanced measures;
- AML/CFT Training;
- Record Keeping Obligations;
- Targeted Financial Sanctions; and
- Suspicious Transaction Monitoring and Reporting

The independent AML/CFT auditor shall be provided access to all records of the Company to enable them to conduct the audit.

The Company shall consider the recommendations and observations of the independent audit report to address any element of non-compliance or improvement of its system and procedures. The Company shall also ensure that appropriate follow-ups are undertaken vis-à-vis the recommendations and observations made by the independent audit function.

The independent audit report shall be filed with the FSC upon the latter's request.

TRAINING

All employees should be made aware of 4XHUB INTERNATIONAL LTD 's Manual.

Employees must be informed of the identity of the MLRO and the Deputy MLRO as well as their responsibilities.

4XHUB INTERNATIONAL LTD needs to ensure that employees who have been provided with the Manual fully understand it and its importance. Employees whose duties relate to the handling of

business relationships or transactions, should especially be made aware of these. These employees should receive AML/CFT related trainings at least once a year or as and when changes to the AML/CFT regime are brought.

Directors, Managers, Legal & Compliance Executives, Compliance Officer, MLRO and DMLRO are considered as relevant employees to whom ongoing training must be given so that they remain competent to give informed and adequate consideration to the evaluation of the effectiveness of the policies, procedures and controls; given that the Board and Senior Management are also responsible for the effectiveness and appropriateness of the Company's policies, procedures and controls to counter money laundering, terrorist and proliferation financing.

Training should be relevant to the role and responsibilities of the employees and may include:

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

There should be a minimum of at least five training sessions annually.

The Company shall further ensure that the Competency Standards as set by the FSC are met at all times.

MONEY LAUNDERING OR OTHER RELATED OFFENCES, AND THEIR SANCTIONS

FIAMLA

- As per Section 8 of the FIAMLA, any person who commits a money laundering offence under Part II of the FIAMLA shall, on conviction, be liable to a fine not exceeding 10 million rupees and to penal servitude for a term not exceeding 20 years.

- As per Section 19 of the FIAMLA, any person who commits an offence relating to the obligation to report and keep records and to disclosure of information prejudicial to a request, shall be liable to a fine not exceeding 10 million rupees and to imprisonment for a term not exceeding 5 years.

FIAML REGULATIONS 2018

- As per Regulation 33 of the FIAML Regulations 2018, any person who commits an offence by contravening these regulations shall be liable to a fine not exceeding 1 million rupees and to imprisonment for a term not exceeding 5 years.

To be noted that the sanctions available to the Enforcement Committee of the FSC to look into breaches include:

- Issuing a private warning;
- Issuing a public censure;
- Disqualifying a Company from holding a licence of a specified kind for a specified period; in the case of an officer, disqualifying the officer from a specified office or position in a Company for a specified period;
- Imposing an administrative penalty; and
- Revoking a licence.

TARGETED FINANCIAL SANCTIONS

Mauritius Sanctions List

The United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 (the 'Act') enables the Government of Mauritius to implement targeted sanctions.

The National Sanctions Secretariat publishes a list of applicable sanctions which must at all times be observed by the Company.

The Company has adopted the policy of not dealing, directly or indirectly, with any sanctioned/designated list persons or country whether or not the dealing may be legitimate or not and whatever the size of the business.

The Compliance screens client's database against sanctions lists issued by the above bodies as well as the sanction list on the internal screening tool of the Company at take-on and on a regular basis via the ongoing monitoring and as for transactions. It is important that any risk of dealing with sanctioned countries or persons by clients is duly escalated to the CEO/Managing Director and MLRO.

Each time the Company receives communique from the Financial Intelligence Unit of any additional or removal, the process is as follows:

- Compliance screens the list from FIU against our client database;
- The list is also screened by Compliance to ensure the screening tool captures these hits;
- A nil report is made on the same or next working day to the FSC and NSS.

Compliance will be responsible to escalate all matters relating to sanctioned persons and countries to management. In addition, Compliance shall be responsible to report to the appropriate authorities and the National Sanctions Secretariat in the appropriate format all cases when there are transactions in accordance to the UN Sanctions Act (or such appropriate guidance).

Screening

4XHUB INTERNATIONAL LTD will screen clients and their related persons at each transaction, at the time of regular review and onboarding. The appropriate checklist will have adequate sections to confirm that screening has been carried out and the results/recommendations thereof.

The screening system used by 4XHUB INTERNATIONAL LTD includes an automated screening for all persons, i.e. all persons which are deemed to be controllers or related persons of the client, to be selected on the system for ongoing screening.

The system will generate a report when there is a hit. Compliance will thereafter review the hit and escalate to the CEO/Managing Director as appropriate for further information. If the hit is not cleared, the CEO/Managing Director will contact the client for further information subject to guidance from Compliance..

4XHUB INTERNATIONAL LTD may perform more regular review of a client subject to a true hit. The client subject to a true hit will be re-rated as high risk. Transaction monitoring will be more robust and intrusive for high-risk clients.

If following a client review and screening, the client becomes high risk, this will be reported to the Compliance Officer. In any other case, Compliance will perform enhanced due diligence which is appropriate to the risk rating and based on the business as well as transactions of the client.

It is apposite that all such results from reviews and actions undertaken following screening reports must be documented, kept on file and adequately recorded.

In accordance with section 23(4) of the Act, any person who holds, controls or has in his custody or possession any funds or other assets of a listed party must, not later than 24 hours of any notice issued under section 18(1) of the Act, notify the National Sanctions Secretariat in writing of:

(a) details of the funds or other assets against which action was taken in accordance with the prohibition to deal with the funds or other assets of a Listed Party;

(b) the name and address of the Listed Party;

(c) details of any attempted transaction involving the funds or other assets, including
- the name and address of the sender;
- the name and address of the intended recipient;
- the purpose of the attempted transaction;
- the origin of the funds or other assets; and
- where the funds or other assets were intended to be sent.

Any person who fails to comply with Section 23 shall commit an offence and shall, on conviction, be liable to a fine not exceeding 5 million rupees or twice the amount of the value of the funds or other assets, whichever is greater, and to imprisonment for a term of not less than 3 years.

Employees

The Company shall ensure that as part of its recruitment process, employees are screened before joining the Company. In instances where due to seniority and responsibility, the prior approval of the FSC is required before employing staff, the Company shall ensure that such approval is obtained.
All relevant employees are required to:

(a) familiarize themselves with guidelines, policies and best practices relating to AML/CFT, as provided for in this Policy;

(b) implement the measures in this Policy diligently and to the best of their ability;

(c) communicate with the Compliance Officer/MLRO for any guidance or clarity required; and

(d) report any suspicious activity to the MLRO.

Adverse Media

Pursuant to the Code of Business Conduct issued under Section 7 (1) (a) of the Financial Services Act 2007, the Company has the duty and obligation to ensure the sound conduct of business and have to establish standards in order to preserve and maintain the good repute of Mauritius as an international financial centre.

If 4XHUB INTERNATIONAL LTD comes across any adverse hits on one of its clients, it shall inform the Commission of the adversely commented press report, and/or public criticism, through prompt submission of a compliance report signed by two directors of 4XHUB INTERNATIONAL LTD .

The procedure for verification upon receipt of sanctions lists from the FIU is as follows:

Step 1: Screening of the lists received to test the screening software to confirm whether hits are captured on the names appearing on the sanctions list.

Step 2: Compliance team tally the lists with the client database. If there is no match, go to step 3. In the contrary, proceed to step 4.

Step 3: Findings are filed.

Step 4: If the name captured relates to one of the clients of 4XHUB INTERNATIONAL LTD , the Compliance Officer will make an internal report to the MLRO.

Step 5: The MLRO will analyse the case and validates the report to the FIU.

SECTION III

OPERATIONS & CORPORATE MANUAL

COMPANIES/TRUSTEES GUIDANCE NOTES

When dealing with clients, in particular companies and/or trusts, 4XHUB INTERNATIONAL LTD must be in a position to adequately assess the associated AML/CFT risks.

WHO IS THE APPLICANT?

When onboarding a company, the applicant refers to the client upon whose instructions the company is being onboarded. This may be a shareholder a director or an authorised signatory.

Where 4XHUB INTERNATIONAL LTD onboard trusts, the applicant will be the settlor(s).

IDENTIFICATION AND VERIFICATION OF IDENTITY

When companies are onboarded, in addition to identifying and verifying the identity of the applicant, 4XHUB INTERNATIONAL LTD must obtain the following:

1. The nature of the company's business and the source of funds

2. Evidence of the identity of each of the principals

Similarly, in the case of a trust being onboarded, 4XHUB INTERNATIONAL LTD must conduct due diligence on all principals involved in the trust. The Company must make appropriate inquiry as to the source of the assets of the settlor which is the trust property. This exercise will vary according to the types of trusts, the trust property and the objectives of the settlor as well as the duration of the trust.

SERVICE PROVIDERS

4XHUB INTERNATIONAL LTD should understand the purposes and activities of their client companies to which they provide services. Suspicion could be raised if 4XHUB INTERNATIONAL LTD is unable to obtain adequate explanation of any of the following features, which may include but is not limited to:

- complex networks of trusts and/or nominee-ships and/or companies
- transactions which are inconsistent (for example, source) with the expected objectives
- arrangements established with the apparent objective of fiscal evasion;
- clarity about beneficial ownership or interests or difficulties in verifying identity of persons with ownership or control;
- unwillingness to disclose the source of assets received by a trust or company.

ONBOARDING STAGE

CLIENT ON-BOARDING

The steps involving client onboarding shall be as follows:

- Following the introductory meeting/first contact with the client, a client profile is established. This includes determining the risk tolerance, return objectives, assessing client's preferences.

- Customer due diligence (CDD) documents are then requested from the client to determine whether they can be onboarded from a CDD perspective. Section 17 of the FIAMLA requires staff members to verify the true identity of all customers and other persons with whom they conduct transactions.

- The company has adopted a system of risk profiling whereby every client is categorized according to the risks that it represents. The due diligence documents to be requested on each type of client is listed in this Manual.

- When conducting due diligence verification on a legal person, verification is done at a minimum on the following:
  a. Promoters
  b. Beneficial owners and ultimate beneficial owners
  c. Officers
  d. Controllers
  e. Company directors
- 4XHUB INTERNATIONAL LTD shall apply CDD measures on all clients. However, in certain particular circumstances where it is deemed that the risk of money laundering is at a minimum, the company will apply simplified due diligence measures. In case the company will apply these reduced CDD measures it shall maintain evidence justifying the application of reduced measures and maintain a record.

- Enhanced due diligence measures shall apply to high-risk business relationship. This type of due diligence will be performed when the Company assesses a certain situation to be of a high-risk nature. Factors that may be considered are the nature of the customer, the business relationship, its location, or any other specificity of the business relationship. Additional steps include request for additional due diligence documents and screening of client.

- At the time of client onboarding, the source of funds of the client (UBO) is also established.

- If all due diligence documents are in order, the client is approved by the Managing Director as well as the Compliance Officer; and, in case of high-risk clients, the MLRO.

- Should the client not meet the CDD verification, the client is declined.

- A discretionary or non-discretionary advisory agreement is then entered between 4XHUB INTERNATIONAL LTD and the client. The agreement will lay out the powers delegated by the client to the Company and its agents in respect of the management of the client's portfolio.

- Once the relationship has been established with the client, 4XHUB INTERNATIONAL LTD will conduct a regular check regarding the relevance of due diligence measures being applied. The ongoing monitoring exercise of the Company consists in the following:
    - Risk profiling review based on events and transactions
    - Questioning complex arrangement of the customers and obtaining evidence of same

- Holding appropriate documentation such as: Investment proof and due diligence documents in case of investments, Agreements, Due diligence documentation on parties with which it interacts in line with its KYC requirements.

The potential client has to complete and sign the Account Opening Form (Refer to Annexure II). Once this is done, the Compliance team has to fill in the Risk Profiling Checklist. This document needs to be verified by the Legal and Compliance team, and approved by the CEO/Managing Director.

4XHUB INTERNATIONAL LTD must undertake CDD measures and be satisfied of the results obtained prior to onboarding any client.

4XHUB INTERNATIONAL LTD may stop at any time the onboarding of client based on non-business-related criteria such as ML/TF and related risks. The decision to reject such clients need not be due to high-risk criteria only but may be due to the behaviour of the client.

Once the onboarding process has been completed, 4XHUB INTERNATIONAL LTD may reject/exit a client due to the following reasons:

1. Residual risk is too high following adverse hits triggered on the client.
2. Onboarding a client may create a conflict of interest with the organisation.
3. There are on-going investigations on the client.
4. ML/TF risks

The decision to reject or off-board a client should be taken together with the MLRO and the CEO/Managing Director and recorded by email.

In case of suspicious transactions or a need to file an STR based on criteria of the FIU, the MLRO shall consider same.

SOURCE OF NEW CLIENT

ELIGIBLE/GROUP INTRODUCER

Eligible Introducer is a person/entity which refers businesses to the Company and is regulated for anti-money laundering purposes or is subject to rules of professional conduct pertaining to anti-money laundering. Eligible Introducers must be either in Mauritius or in a jurisdiction that has in place anti-money laundering legislation that is at least equivalent to the legislation in Mauritius.

Group Introducer is an entity that is part of the same group as the Licensee and is subject for anti-money laundering purposes either to the consolidated supervision of a regulator in Mauritius or in an equivalent jurisdiction or is subject to the anti-money laundering regulation of a regulator in Mauritius or in an equivalent jurisdiction.

All Eligible/Group Introducers have to sign an Agreement (Memorandum of Understanding, Partnership Agreement or Referral agreement) with 4XHUB INTERNATIONAL LTD . These Agreements defer in names only as per the jurisdictions where the introducers are based. Such Agreements are kept under the safe custody of 4XHUB INTERNATIONAL LTD ’s Compliance Department. A full KYC check of the Eligible/Group Introducers needs to be done by the said department.

At the time of establishing the introducer relationship, the Company shall carry out a risk analysis of this relationship which should then be monitored.

4XHUB INTERNATIONAL LTD does not accept CDD carried out by an Eligible Introducer.

The risk of money laundering to 4XHUB INTERNATIONAL LTD is not posed solely by future client relationship. Existing clients can also pose significant risks. 4XHUB INTERNATIONAL LTD need to assess the risk of its client base and the extent and nature of the client due diligence information held or of any additional documentation or information that may be required for existing clients in accordance with the criteria within the FSC Handbook on AML/CFT.

4XHUB INTERNATIONAL LTD must apply CDD requirements to existing clients on the basis of materiality and risk and conduct due diligence on such existing relationships when necessary.

Below are examples of situations where it is desirable to conduct CDD checks on existing clients. Please note that this list is by no means prescriptive:

1. a transaction of significance amount takes place,
2. client documentation standards change substantially,
3. there is a material change in the way the account is operated,
4. eligible introducer becomes aware that it lacks sufficient CDD information about an existing client.

CLIENT DUE DILIGENCE MEASURES – 'CDD MEASURES'

As a matter of internal policy, the full range of CDD measures should be applicable using a risk-based approach as provided for in our Risk Profiling Checklist. CDD measures include:

- Identifying and verifying the identity of the applicant using reliable, independent source documents, data or information;

- Identifying and verifying the identity of the beneficial owner (ultimate owner), such that the Company is satisfied that it knows who the beneficial owner is. Note: FSC regards the beneficial owner as the natural person(s) who ultimately own(s) or control(s) a client and/or the person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement;

- Obtaining information on the purpose and intended nature of the business relationship; and

- Conducting ongoing due diligence on the business relationship and scrutiny of transactions throughout the course of the business relationship with eligible introducer's knowledge of the client and his business and risk profile (including the source of funds).

IDENTIFICATION AND VERIFICATION OF APPLICANTS WHO ARE NATURAL PERSONS

IDENTIFICATION DATA FOR NATURAL PERSONS

eligible introducer must collect relevant identification data on a natural person, which includes:

- Name (including any former names, any other names used and other aliases)
- Current residential address
- Date and place of birth
- Nationality

VERIFICATION OF IDENTITY OF NATURAL PERSONS

(a) Verification of the identity of the natural person

The following types of identity documentation can be relied upon:

- National Identity cards
- Current valid passports

(b) Verification of the address of the natural person

The following identity documentation can be relied upon to verify the address of the applicant if he/she is a natural person:

- A recent utility bill issued; not later than 3 months
- A recent bank or credit card statement dated; or ▪ A recent bank reference.

Alternatively, verification may be achieved by:

- Obtaining a reference from a professional person who knows the natural person. The reference must include the permanent residential address of the individual;
- Checking a current register of electors;
- Utilizing an address verification service; or
- Visit the individual at his/her current residential address.

IDENTIFICATION AND VERIFICATION OF APPLICANTS WHO ARE LEGAL PERSONS/ARRANGEMENTS

LEGAL PERSONS

Legal persons include bodies corporate, partnerships, associations or any other body of persons other than legal arrangements.

VERIFICATION OF THE EXISTENCE OF A LEGAL PERSON AND IDENTIFYING THE PRINCIPALS THEREOF

Where an applicant is a legal person, 4XHUB INTERNATIONAL LTD must –

- take reasonable measures to understand the ownership and control structure of the applicant;
- verify and establish the existence of the legal person; and
- determine the identity of the principals of the legal person.

For avoidance of doubt, in the case of a legal person, principals of applicants for business include the following:

- Promoters
- Beneficial owners and ultimate beneficial owners
- Officers
- Controllers
- Company Directors

4XHUB INTERNATIONAL LTD **must:**

- identify and verify the identity of the legal person, including name, incorporation number, date and country of incorporation or registration;

- identify and verify any registered office address and principal place of business (where different from the registered office);

- verify the legal status of the legal person; and

- identify and verify the identity of underlying principal (including beneficial owners, controllers, directors or equivalent) with ultimate effective control over the capital or assets of the legal person; and

- verify that any person who purports to act on behalf of the legal person is duly authorized and identify that person.

Where the underlying principals are not natural persons, 4XHUB INTERNATIONAL LTD must 'drill down' to establish the identity of the natural persons ultimately owning or controlling the business.

PRIVATE COMPANIES

- Obtaining an original or appropriately certified copy of the certificate of incorporation or registration;

- Checking with the relevant companies' registry that the company continues to exist;
- Reviewing a copy of the latest report and accounts if available (audited, where possible);
- Obtaining details of the registered office and place of business;
- Verifying the identity of the principals of the company as above;

LEGAL ARRANGEMENTS

Trusts do not have separate legal personality and therefore form business relationships through their business. It is the trustee of the trust who will enter into a business relationship on behalf of the trust and should be considered along with the trust as the client.

VERIFICATION OF THE EXISTENCE OF A LEGAL ARRANGEMENT AND IDENTIFYING THE PRINCIPALS THEREOF

Where an applicant is a legal arrangement, 4XHUB INTERNATIONAL LTD must –

- take reasonable measures to understand the ownership and control structure of the applicant;
- verify and establish the existence of the legal arrangement; and
- determine the identity of the principals of the legal arrangement.

For avoidance of doubt, in the case of a legal arrangement, principals of applicants for business include the following:

- Settlors or Contributors of capital (whether named or otherwise)
- Trustees
- Beneficiaries
- Protectors
- Enforcers

4XHUB INTERNATIONAL LTD **must:**

1. verify the legal status of the legal arrangement;

2. identify and verify the identity of the principals of the applicant, that is, those natural persons with a controlling interest and those who comprise the mind and management of the legal arrangement; and

3. obtain information concerning the name of trustee(s), its legal form, address and provisions binding the legal arrangement.

In relation to a trust, the above requirements can be achieved by:

- Obtaining an original or appropriately certified copy of the trust deed or pertinent extracts thereof;
- Where the trust is registered – checking with the relevant registry to ensure that the trust does exist;
- Obtaining details of the registered office and place of business of the trustee; ▪ Verifying the identity of the principals of the trustee as above.

ACQUISITION OF A BUSINESS OR BLOCK OF CLIENTS

There are circumstances where 4XHUB INTERNATIONAL LTD may acquire business with established business relationships or a block of clients. Before taking on such type of business, 4XHUB INTERNATIONAL LTD should undertake sufficient enquiries to determine whether the CDD policies, procedures and controls as described in the Procedure Manual of the other Licensee is satisfactory and in line with prevailing legislations to establish the level and the appropriateness of identification data held in relation to the clients and the business relationships of the business to be acquired.

4XHUB INTERNATIONAL LTD may rely on the information and documentation previously obtained where:

- the business relationships were established in jurisdictions with no deficiency in AML/CFT;
- the CDD policies, procedures and controls which were in place were satisfactory; and
- 4XHUB INTERNATIONAL LTD has obtained identification data for each client acquired.

Where deficiencies in the identification data held are identified (either at the time of transfer or subsequently), the accepting Licensee, that is, 4XHUB INTERNATIONAL LTD , must determine and implement a program to remedy any such deficiencies.

SOURCE OF FUNDS/PROPERTY AND SOURCE OF WEALTH

In the identification of risk and prevention of money laundering, it is a pre-requisite for 4XHUB INTERNATIONAL LTD to understand the origin or provenance of funds when establishing business relationship with a client. Therefore, understanding the client's source of funds and the client's source of wealth is an important aspect of client due diligence.

It is important to distinguish between the source of funds and the source of wealth. The "source of funds" is the activity or transaction which generates the funds for a client while the "source of wealth" refers to the activities which have generated the total net worth of the client.

4XHUB INTERNATIONAL LTD must therefore use a risk-based approach and by taking appropriate measures establish the source of funds for each applicant.

SIGNATURE OF CLIENT AGREEMENT

The client agreement should be signed by the client or if a corporate client, by a director or an authorised representative.

CERTIFICATIONS

Section 17of the FIAMLA:

(1) "Every reporting person shall –

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

Where reliance is placed upon verification of identity documents, the latter have to be certified as true copies of the original documents (if not in original form) by an approved certifier.

Note that where an employee of 4XHUB INTERNATIONAL LTD meets an applicant or the principals thereof face-to-face and has access to original verification of identity documentation, he or she may take copies of the verification of identity documentation and certify them personally as true copies of the original documentation.

Copies of the verification of identity documentation can be certified by a suitable person, for instance,

1. a lawyer;
2. a notary;
3. an actuary;
4. an accountant or any other person holding a recognised professional qualification;
5. a director or secretary of a regulated financial institution in Mauritius or in equivalent jurisdiction; or
6. a member of the judiciary or a senior civil servant.

This list of suitable certifiers is not exhaustive and 4XHUB INTERNATIONAL LTD employees must exercise due caution when considering certified copy documents, especially where such documents originate from a country perceived to represent a high risk, or from unregulated entities in any jurisdiction. The suitable certifier should sign the copy document and clearly indicate, the following:

"I hereby certify that this is a true copy of the original document.
Signature of Certifier: _____
Full Name of Certifier: _____
Capacity of Certifier: _____
Date of Certification: _____
Address of Certifier: _____
Contact Details of Certifier: _____"

Where certified copy documents are accepted, it is 4XHUB INTERNATIONAL LTD 's responsibility to ensure that the certifier is appropriate. In all cases, the Company should ensure that the client's

signature on the identification documents matches the signature on the application form, mandate or other document.

TIMING OF VERIFICATIONS

4XHUB INTERNATIONAL LTD must take all reasonable measures to complete all CDD measures for all applicants prior to onboarding a new client.

The CDD measures must in any event be satisfactorily completed, such that: -

a. it occurs as soon as reasonably practicable;
b. it is essential not to interrupt the normal conduct of business;
c. the money laundering risks are effectively managed.

4XHUB INTERNATIONAL LTD has appropriate and effective policies, procedures and controls in place, so as to manage the risk, which include:

a. establishing that this is not a high-risk relationship;
b. monitoring by senior management of these business relationships to ensure that the verification of identity is completed as soon as reasonably practicable;
c. ensuring funds received are not passed on to third parties;
d. monitoring large transactions.

In the event that satisfactory CDD documentation has not been obtained, 4XHUB INTERNATIONAL LTD has procedures in place to disengage from or terminate such business relationships. 4XHUB INTERNATIONAL LTD should consider the potential risks inherent in engaging in any form of relationship with any applicant prior to satisfactorily completing CDD measures.

If the Company is unable to:

- establish and verify the identity of a customer or other relevant person;
- obtain information to understand the nature and intended purpose of the business relationship and source of funds; or

- conduct on-going due diligence,

the Company:

- may not establish a business relationship or conclude a single transaction with a customer;
- may not conclude a transaction in the course of a business relationship, or perform any act to give effect to a single transaction;

and must terminate an existing business relationship with a customer. The Company shall also consider submitting an STR if the circumstances which prevent the Company from conducting customer due diligence are suspicious or unusual.

RISK PROFILING

After the collection of the CDD documentation, 4XHUB INTERNATIONAL LTD must make an initial assessment of the risk to which the business relationship will expose it and evaluate the client accordingly. In this exercise, 4XHUB INTERNATIONAL LTD will take into consideration a number of factors, including but not limited to the following:

- The nature and type of client
- The geographical location of the client's residence
- The geographical location of the client's business interests and/or assets
- The nature and value of the assets concerned in the relationship
- The client's source of funds and where necessary the source of wealth
- The role of any introducer and the introducer's regulated or professional status

4XHUB INTERNATIONAL LTD must routinely consider the risks that all relationships pose to them and the manner in which those risks can be limited. To do so, 4XHUB INTERNATIONAL LTD must be able to demonstrate the effective use of documented CDD information. If 4XHUB INTERNATIONAL LTD does not 'know a client', it will not be in a position to recognize and manage the risks inherent to the relationship.

On-going monitoring of client transactions and on-going reviews are fundamental components of an appropriate risk-based assessment.

In terms of risk weightage, the Company should ensure that there is no undue influence on the weightage by one single risk factor. Further, financial considerations should also not influence the ratings.

The risk rating generated post the assessment will determine the frequency of the review which the Company should carry out.

The Company shall further review its customer risk profiling methodology to ensure the customer risk categories remain relevant and reflective of the real risk that the Company is exposed to as a result of its customer relationships.

As with the business risk assessment, the client risk assessments, need to be comprehensively documented with the rationale for decisions being clearly explained and recorded.

LOW RISK RELATIONSHIP

In general, the full range of CDD measures should be applied to all applicants. However, where the risk of money laundering or the financing of terrorism is lower and where information on the identity of the applicant is publicly available or where adequate checks and controls exist elsewhere in the national systems, it might be reasonable for 4XHUB INTERNATIONAL LTD to apply simplified or reduced due diligence measures when identifying and verifying the identity of the applicant 4XHUB INTERNATIONAL LTD .

4XHUB INTERNATIONAL LTD must ensure that when they become aware of circumstances which affect the assessed risk of the business relationship or occasional transaction, they must undertake a review of the CDD documentation and information held with a view to determine whether it is appropriate to continue applying simplified or reduced CDD measures.

Where 4XHUB INTERNATIONAL LTD take a decision to apply simplified or reduced CDD measures, documentary evidence which supports the decision must be retained.

However, simplified CDD measures will not be acceptable whenever there is suspicion of money laundering or terrorist financing or specific higher risk scenarios apply.

Where any aspect of the relationship exposes 4XHUB INTERNATIONAL LTD to an increased level of risk, then simplified or reduced CDD measures must not be applied.

Frequency of review for all low risk clients shall be every 24 months.

MEDIUM RISK RELATIONSHIP

4XHUB INTERNATIONAL LTD will apply standard CDD measures as required under the FIAML Regulations and the AML-CFT Handbook where it has assessed that the business relationship or occasional transaction is a medium-risk relationship, based on the client's individual risk status, that is, the nature of the client, the business relationship, its location, or any other specificity of the business relationship.

Frequency of review for all Medium risk clients shall be every 18 months.

HIGH RISK RELATIONSHIP

4XHUB INTERNATIONAL LTD will apply enhanced CDD measures as required under Regulation **25(1)** of the FIAML Regulations where it has assessed that the business relationship or occasional transaction is a high-risk relationship, based on the client's individual risk status, that is, the nature of the client, the business relationship, its location, or any other specificity of the business relationship.

Frequency of review for all high risk clients shall be every 12 months.

FATF STATEMENTS AND NON-COOPERATIVE JURISDICTIONS

When designing the internal procedures, 4XHUB INTERNATIONAL LTD had regard to the need for enhanced due diligence and additional monitoring procedures for transactions and business relationships involving countries which are non-cooperative jurisdictions or which have been the subject of FATF Public Statements for deficiencies in their AML/CFT systems.

CONCLUSION

4XHUB INTERNATIONAL LTD has accordingly devised a comprehensive compliance procedure regarding the above, and same is reflected in our Risk Profiling Sheet.

ENHANCED DUE DILIGENCE

Enhanced due diligence, would imply taking additional steps in relation to identification and verification. This may include the following steps:

- obtaining further client due diligence information (identification and relationship information) from either the client or independent sources (such as the internet, public or commercially available databases);
- verifying additional aspects of the client due diligence information obtained;
- taking appropriate and reasonable measures to establish the source of the funds and the wealth of the client, any beneficial owner and underlying principal; and
- carrying out more frequent and more extensive ongoing monitoring on such business relationships with setting lower monitoring thresholds for transactions connected with such client.

USE OF THIRD PARTIES

4XHUB INTERNATIONAL LTD may use the services of third parties for the provision of services in relation to its business activity. These service providers will be engaged following a meeting of Senior Management, after taking into consideration, the risks that may be posed to 4XHUB INTERNATIONAL LTD .

Such third-party service providers should be assessed in terms of their experience and track record to provide the services as well as their CDD.

4XHUB INTERNATIONAL LTD will not use third parties for conducting CDD. 4XHUB INTERNATIONAL LTD will always conduct its own CDD but may rely on another person to channel CDD information only especially when there is a person or related company acting as intermediary. These persons will not be used as eligible introducers.

Any intermediary should be subject to appropriate CDD and screening measures for clients every time they act as such for a new client.

POLITICALLY EXPOSED PERSONS (PEPS)

Regulation 2 of the FIAMLR defines a foreign PEP, a domestic PEP and an international organisation PEP as follows:

Domestic PEPs - individuals who are or have been entrusted domestically with prominent public functions in Mauritius and includes the Head of State and of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.

Foreign PEPs – individuals who are or have been entrusted with prominent public functions by a foreign country, including Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.

International organisation PEPs – individuals who are or have been entrusted with a prominent function by an international organisation and includes members of senior management such as directors, deputy directors and members of the board or equivalent functions.

Family members PEPs – are individuals who are related to a PEP either directly (consanguinity) or through marriage or similar (civil) forms of partnership. Family members & close associates of PEPs should be determined to be PEPs because of the potential for abuse of relationship for the purpose of Money Laundering& Terrorism Financing (ML&TF).

Close associates of PEPs are individuals who are closely connected to a PEP, either socially or professionally and as such are also deemed PEP.

PEPs are individuals who are or who have been entrusted with prominent public functions (for example Heads of State or of Government, Senior Politicians, Senior Government, Judicial or Military Officials, Senior Executives of State-Owned Corporations and important Political Party Officials, their immediate family members and close associates).

The company should be aware that business relationships with PEPs, family members or close associates of PEPs are deemed to pose a greater than normal money laundering risk by virtue of the possibility for them to have benefited from proceeds of corruption.

The company should thus take additional measures when dealing with such individuals as any scandal associated to them can have major repercussions on their business partners.

Therefore, the company has put in place a policy for the onboarding of these PEPs. The following steps should be followed by the Administrator or company when a PEP is identified or there are any high risk individuals or entities. All PEPs shall be recorded in the Register of PEPs.

Step 1: Collect all due diligence documents on the persons.

Step 2: Perform screening.

If screening is clear or does not contain any adverse information move to step 3. On the contrary move to step 4.

Step 3: Provide the Compliance Officer with the screening and due diligence documents so that further internet search can be conducted. If no adverse results are found on the person and all due diligence documents are in order, seek the approval of senior management before accepting the client.

Step 4: Provide the Compliance Officer with the screening and due diligence documents so that further internet search can be conducted. Irrespective if further adverse results are found on the internet, The Compliance Officer will prepare a detailed report with recommendations for senior management to consider approving the onboarding of the PEP.

Step 5: Request further documents or information as approved by the Board.

Step 6: Upon receipt of the information and documents, provide compliance.

PEP related clients will be classified as high risk and the measures applying to a high risk client should be followed.

4XHUB INTERNATIONAL LTD must ensure to:

- obtain the approval of Senior Management prior to establishing relationships with such applicants for business;

- where applicants have been accepted and the said applicant or its beneficial owner is subsequently found to be, or subsequently becomes, a PEP, obtain the approval of Senior Management to continue such business relationships;

- obtain similar approval from Senior Management in cases of family members or close associates of PEPs;

- take enhanced due diligence measures to establish the source of funds and source of wealth of applicants, beneficial owners, family members or close associates of PEPs;

- conduct enhanced ongoing monitoring of the business relationships involving PEPs, family members or close associates of PEPs (including Connected Persons).

4XHUB INTERNATIONAL LTD must apply appropriate EDD measures on a risk-sensitive basis where an applicant or customer (or any connected person, such as a beneficial owner or controller) is a PEP.

4XHUB INTERNATIONAL LTD shall apply the same measures for CDD and monitoring in relation to Connected Person as for PEPs.

4XHUB INTERNATIONAL LTD shall rely on screening systems to determine relationships with non-domestic PEPs and Google searches for local PEPs given that there is no repository for local PEPs.

In the event of doubt, 4XHUB INTERNATIONAL LTD may request the services of a third party to perform further checks to determine whether a person is a PEP.

The risks associated with PEPs differ according to the particular countries concerned. The risk of corruption in certain countries is higher than it is in others. 4XHUB INTERNATIONAL LTD do take note of the Transparency International Corruption Perceptions Index at www.transparency.org and take appropriate measures to manage the increased risks of conducting business with PEPs.

When accepting a PEP client, the PEP register will have to be updated.

NON-FACE TO FACE BUSINESS RELATIONSHIP

The FSC recognizes that the business conducted by 4XHUB INTERNATIONAL LTD may also be conducted on a non-face to face basis with clients. Often, it is either impossible or impractical for 4XHUB INTERNATIONAL LTD to have or to obtain original documentary evidence of identity. However, in such cases, 4XHUB INTERNATIONAL LTD should apply the following CDD procedures when dealing with non-face to face applicants for business:

- the certification of documents presented;
- the requisition of additional documents to complement those which are required for face to face applicant; and
- the initiation of an independent contact with the client.

ONGOING MONITORING

The Client Services team has to conduct a review of each client file based on their risk rating and any issue raised should be submitted to the Compliance Department.

For example, in relation to the source of funds, the following questions might be asked when determining whether incoming funds may be suspicious:

- Is the volume and/or size of the transactions consistent with the normal pattern of activity for the client?

- Is the receipt of the transaction in the context of the client's business or personal activities and their stated commercial objectives?

The risk rating awarded to the client determines the frequency of review by the Legal & Compliance Department as follows:

- Every twelve months for High Risk rated clients

- Every eighteen months for Medium Risk rated clients

- Every twenty-four months for Low Risk rated client

In such cases the Client Services Department should follow up for any outstanding issues as soon as it is made aware of compliance discrepancies (if any), within the appropriate ongoing monitoring time frame.

In the event that clients are not responding to any query or communications or there is a tendency from clients to ignore regulatory/statutory duties or events, the matter must be escalated to the CEO/Managing Director and Compliance as soon as practicable and to prevent any regulatory issue from impacting the Company.

In this event, the CEO/Managing Director will, based on information available and final requests to client, decide on the next steps including resignation in statutory roles and inform the regulator or authorities.

TERMINATION OF AGREEMENT WITH CLIENT

If the client wishes to terminate the Agreement with the Company, the client should formally inform the company in writing. The records of the client will be kept for a period of 7 years.

COMPLIANCE POLICIES

GIFT, ENTERTAINMENT OR BENEFIT POLICY

4XHUB INTERNATIONAL LTD staff must not directly or indirectly solicit a gift, entertainment or benefit, from any Client or business related third party, for their benefit or for the benefit of others. 4XHUB INTERNATIONAL LTD staff should not put themselves in a position where it could appear that their independence or judgment has been compromised by the acceptance of any such gift, entertainment or benefit. Any gift, entertainment or benefit received must not give rise to a conflict of interest.

Cash gifts should NOT be accepted in any circumstances. In principle, gifts, entertainment or benefits of MUR 200 (Mauritian Rupees Two Hundred) or above must be disclosed to the Legal & Compliance Department by completing the Gift, Entertainment or Benefit Disclosure Form. The estimation of the gift, entertainment or benefit should be as per the current conversion rate.

RECORD KEEPING POLICY

4XHUB INTERNATIONAL LTD keeps all records in relation to its activities as required by the law. Records comprise of full and true written details of every transaction that the company conducts:

The records are kept:

- In physical form or electronic data storage in the computers' hard disc;
- For a period of at least 7 years after the completion of the transaction to which it relates;
- At the registered office of 4XHUB INTERNATIONAL LTD or such other place as may be agreed; and
- For identification purposes as per the index of each file.

Pursuant to section 17F of FIAMLA 2002, 4XHUB INTERNATIONAL LTD must keep such records, registers and documents as prescribed in Regulation **17F(2)** of the FIAML Regulations 2018.Furthermore section 29 of the Financial Services Act 2007 requires 4XHUB INTERNATIONAL LTD to keep and maintain internal records of the identity of each Customer as well as full and true written records of all transactions relating to his business activities.

4XHUB INTERNATIONAL LTD is also required to maintain the following records on the suspicious reports being filed:

- The internal suspicion reports received by the MLRO;
- Records of action taken under the internal and external reporting requirements;
- When the MLRO has considered information or other material concerning the reports, but has not made a disclosure of suspicion to the FIU, a record of the information or material that was considered and the reason for the decision; and
- All reports made by the MLRO to the FIU.

4XHUB INTERNATIONAL LTD is also required to maintain records of all AML/CFT training delivered to employees. Records should include:

- The dates AML/CFT training was provided;
- The nature of the training, including details of contents and mode of delivery; and
- The names of the employees who received training.

CONFLICT OF INTEREST POLICY

A conflict of interest arises when any director, shareholder or employee of the Company unfairly places his/her interests above those of the client. The Company should place the client's interests above its own, thus meeting the reasonable expectation of a properly informed client.

4XHUB INTERNATIONAL LTD ensures to take reasonable steps to avoid a conflict of interest arising or, where conflicts arise, shall ensure fair treatment for all its clients by full disclosure of material facts, internal rules of confidentiality, declining to act or otherwise.

ADDRESSING CONFLICTS OF INTEREST

In order to gain the confidence of the authorities as to its objectivity and impartiality, rules and procedures is established by the Company to guarantee that:

- Conflicts of interest are treated in a lawful and ethical way;

- In the conduct of their duties, directors and employees of the Company:

  - will arrange their private affairs in a manner that will prevent real, apparent or potential conflicts of interest from arising;
  - will not solicit or accept transfers of economic benefit;
  - will not step out of their roles to assist other outside entities or third parties in their dealings where this would result in a preferential treatment to the latter;
  - will not knowingly take advantage of, or benefit from, any information that is obtained in the course of their official duties;

Where 4XHUB INTERNATIONAL LTD has a material interest in a transaction to be entered into with or for a client, or a relationship which gives rise to a conflict of interest in relation to such a transaction, 4XHUB INTERNATIONAL LTD shall not knowingly either advise, deal or otherwise act in relation to that transaction or relationship unless it has:

a. fairly disclosed that material interest or relationship, as the case may be to the client; or

b. taken reasonable steps to ensure that neither the material interest nor relationship adversely affect the interests of the client.

In order to minimize potential conflicts of interests, 4XHUB INTERNATIONAL LTD will clearly disclose all identified sources of conflicts to the client, before the latter enters into any contractual relationship with the company.

A conflict of interest register is maintained by the Legal & Compliance Department detailing all conflicts of interest including:

- all conflicts of interest notification;
- any reported cases of failure to disclose;
- disclosure by others, such as colleagues or clients;
- assessment of the matter and how it was considered;
- any action taken; and
- any reviews of the assessment process.

The information recorded in the register and documents evidencing the conflict of interest are kept for at least 7 years.

TRANSACTION MONITORING POLICY

The Company shall monitor its business relations with clients on an ongoing basis and observe the conduct of clients' activities and transactions to ensure that they are consistent with its knowledge of the client, its business and risk profile and where appropriate, the source of funds.

The ongoing monitoring of clients' activities and transactions, is a fundamental aspect of effective ongoing CDD measures in the identification and mitigation of money laundering, terrorist and proliferation financing risks.

Transaction Monitoring is a process put in place to monitor all transactions and activity of the Company on an ongoing basis, which involves a combination of real-time and post-event monitoring. In the case of real time monitoring, the focus is on transactions/activity where information/instructions are received before a payment instruction is processed. Post-event monitoring consists of reviewing transactions/activity on a periodic basis (e.g. monthly).

The over-riding principle is to ensure that unusual transactions and activity are identified and subject to a heightened level of scrutiny or examination within the shortest delay and properly documented. Where the risks of money laundering, terrorism or proliferation financing are higher, enhanced CDD measures must be conducted which are consistent with the risks identified. Of note, transaction monitoring can trigger an Internal Investigation and warrant a STR report, in case a suspicious transaction is identified.

Transactions will be rated as either of these:

1. **Level 1 - Low Risk**

Transactions below a threshold of USD 7,500 or its equivalent in foreign currency will be classified as Low Risk.

2. **Level 2 - Medium Risk**

Transactions exceeding a threshold of USD 7,500 or its equivalent, but below that of USD 50,000 or its equivalent will be classified as Medium Risk.

3. **Level 3 - High Risk**

Transactions exceeding a threshold of USD 50,000 or its equivalent will be classified as High Risk.

Irrespective of the above classifications and amount, transactions will be classified as high-risk if:

- Transactions involving clients rated as ‘High Risk’
- Transactions involving PEP clients
- Transactions where transfer instructions and other communications were received from an email address different from that initially provided by the client.

PROCEDURE FOR TRANSACTION MONITORING

1. After client onboarding, the client will deposit funds into the client account of the company.
2. The Transaction Monitoring Executive will ensure that all CDD documents and evidence of screenings and source of funds are on file.
3. The Transaction Monitoring Executive will go through the bank statement/ any platform set up by the Company on a daily basis regarding inflow and outflow of funds.
4. If need be, additional documentations will be requested or client will be queried.

ANNEXURE I
INDICATORS OF POTENTIALLY SUSPICIOUS ACTIVITY

1. Any doubt over the true identity of an applicant or the principals thereof

2. Any unusual transaction in the context of the normal pattern of activity for a particular relationship

3. Reluctance on the part of clients to respond to enquiries made by Licensee

4. Fund transfers to or from accounts in countries that are known to be associated with drug trafficking or other serious crime

5. Clients who produce or demand for collecting large quantities of cash

ANNEXURE II