Xtream Markets LTD

Policies and Procedures Manual 2023

Fiduciary Statement

Background

The Company holds a Global Business License ("GBL") issued by the FSC on 08 March 2023 as well as an Investment Dealer (Full Service Dealer excluding Underwriting) license (the "ID License") granted by the FSC on 08 March 2023.

An investment dealer has an affirmative duty to act in the best interests of its clients and to make full and fair disclosure of all material facts to the exclusion of any contrary interest. Generally, facts are "material" if a reasonable investor would consider them to be important. The duty of addressing and disclosing conflicts of interest is an ongoing process and as the nature of an investment dealer's business changes, so does the relationship with its clients.

The Company will be both acting as an intermediary in the execution of securities transactions for clients and will also be dealing on own account, that is trade in securities as principal with the intention of reselling these securities to the public. The Company will deal in the following financial instruments:

a) CFDs Currency Pairs,

b) CFDs Future Indices,

c) CFDs Spot/Cash Indices,

d) CFDs Metals,

e) CFDs Commodities/Energies.

(i) Executing orders for clients

The Company receives clients' orders and the Company automatically creates and sends new orders for Execution to its Liquidity Providers ('LPs'). Once the Company receives a confirmation from the LP about the execution of the order, it automatically sends a confirmation to the client's order originally received. The prices provided to clients include the Company's mark-up. The Company applies mark-ups on spread, commissions and swaps based on the quotes received from the liquidity providers that it cooperates with. The Company will have access to a range of liquidity providers and depending on the trade direction, size, and market condition it will direct trades accordingly in order to offer the best possible execution of order based on likelihood, price, cost, speed and other related factors as per its business plan. At the initial stage of the Company's operations, the Company will establish a business relationship with one Liquidity Provider as stated in its business plan.

Where the Company acts as intermediary then the Company has always zero exposure as the exposure with clients is netted off versus the exposures with LPs.

(ii) Trade in securities as principal with the intention of reselling these securities to the public

The Company will sometimes be the counterparty of the clients' orders i.e. will be making profit / loss from trading activity when clients make loss / profit. When the Company receives clients' orders and provided these are within accepted risk management limits (as decided by the Board of Di-rectors), the Company sends a confirmation to the clients without hedging the clients' orders with Liquidity Providers

in addition, the Company shall always comply with section 56(3) and (4) of the Securities Act 2005. In this respect, the Company shall not trade as principal in securities listed or traded on a securities exchange except in accordance with the applicable rules of the securities exchange. Where, in respect of securities that are not listed on a securities exchange, where the Company will be acting as principal with a client, the Company shall, before entering into the transaction, disclose to the client that it is entering into the transaction as principal

Company Statement

As an investment dealer, XTREAM MARKETS LTD (hereinafter "XML" or the "Company") owes its clients specific duties of a fiduciary nature:

- Provide advice that is suitable for the client;
- Give full disclosure of all material facts and any potential conflicts of interest to clients and prospective clients;
- Serve with loyalty and in utmost good faith;
- Exercise reasonable care to avoid misleading a client; and
- Make all efforts to ensure best execution of transaction

XML seeks to protect the interest of each client and to consistently place the client's interests first and foremost in all situations. It is the belief of XML, as an investment dealer, that its policies and procedures are sufficient to prevent and detect any violations of regulatory requirements as well as the Company's own policies and procedures

Compliance Officer Appointment

The person herein named "Compliance Officer" is stated to be competent and knowledgeable regarding the applicable rules and regulations and is empowered with full responsibility and authority to develop and enforce appropriate policies and procedures for the Company. The Compliance Officer ("Compliance Officer" or "CO") has a position of sufficient seniority and authority within the organization to compel others to adhere to the compliance policies and procedures.

Compliance Officer	Date Responsibility
Assumed Kishen Kumar Hurhinidee	08 March 2023

Code of Ethics Statement

Background

In accordance with regulations, XML has adopted a code of ethics to:

- Set forth standards of conduct expected of advisory personnel (including compliance with securities laws);
- Safeguard material non-public information about client transactions; and
- Require "access persons" to report their personal securities transactions.

Introduction

As a holder of the ID License, the Company has an overarching fiduciary duty towards its clients, whose interests come first. The Company has an obligation to uphold that fiduciary duty and see that its personnel do not take inappropriate advantage of their positions and the access to information that comes with their positions.

XML holds its directors, officers, and employees accountable for adhering to and advocating the following general standards to the best of their knowledge and ability:

l. XML shall observe and comply with all relevant laws wherever they operate.

2. XML shall observe and comply with the spirit as well as the letter of the regulations prescribed by the FSC.

3. XML shall cooperate with all responsible authorities in the jurisdictions where it operates.

4. XML shall act in a manner which recognizes that integrity and responsibility are essential to win and maintain the confidence of XML of the public in all aspects of the securities industry.

5. XML shall conduct its business in a professional manner and in accordance with sound business practice

6. XML shall ensure that its staff are thoroughly and appropriately trained, knowledgeable and competent in all aspects of the securities industry which are relevant to the proper performance of their duties and responsibilities.

7. XML shall ensure that all its relevant staff obtain registration (where applicable) under relevant regulations.

8. XML shall respect and preserve the confidentiality of its clients.

9. XML shall not use information provided by clients which has not been made public for its own or others benefit as this may amount to insider dealing.

10. XML shall ensure that the overriding principle in carrying out its activities is the benefit and interest of clients.

11. XML shall not issue misleading advertisements intrude upon the privacy of the public through door-to-door canvassing or other similar methods.

12. XML shall provide clients with all requisite documentation promptly in accordance with their stated intentions.

13. XML shall abide by all policies and statements of intention stated in its documentation and shall ensure that clients and potential clients are given adequate warning of any proposed changes of intention or policy.

14. 14. XML shall not engage in any professional conduct involving dishonesty, fraud, deceit or misrepresentation commit any act that reflects adversely on its honesty, trustworthiness professional competence.

15. The Code of Ethics will be binding on all officers, advisers, managers and employees of XML.

16. Professional misconduct in the nature of misrepresentation and fraudulent, dishonest or misleading conduct by any officer, adviser, manager or employee of XML will result in disciplinary action and prosecution where applicable.

17. Failure to comply with XML's Code of Ethics may result in disciplinary action, up to and including termination of employment.

Prohibited Purchases and Sales

Insider Trading

Illegal insider trading refers generally to buying or selling a security, in breach of a fiduciary duty or other relationship of trust and confidence, while in possession of material, nonpublic information about the security. Information is material if 'there is a substan-tial likelihood that a reasonable shareholder would consider it important' in making an investment decision. Information is nonpublic if it has not been disseminated in a manner making it available to investors generally.

XML strictly prohibits trading personally or on the behalf of others, directly or indirectly, based on the use of material, non-public or confidential information, XML additionally prohibits the communicating of material non- public information to others in violation of the law. Employees who are aware of the misuse of material nonpublic information should report such to the Risks and Complaints Officer of the Company (the "RCO Muhammad Sohail Safdar Email: complaints@xtreamforex.com), This policy applies to all of XML's employees. and associated persons without exception.

The RCO collects and maintains a list of each access persons personal securities owned. The RCO reviews the summaries for inap-propriate transactions and report them to the CEO for action. Access persons report their personal securities transactions on at least a quarterly basis and annually thereafter.

Prohibited Activities.

Conflicts of Interest Policy

XML has an affirmative duty of care, loyalty, honesty, and good faith to act in the best interest of its clients. All supervised persons must refrain from engaging in any activity or having a personal interest that presents a "conflict of interest. A conflict of interest may arise if the supervised person's personal interest interferes, or appears to interfere, with the interests of XML or its clients. A conflict of interest can arise whenever supervised person takes action or have an interest that makes it difficult for him/her to perform his/her duties and responsibilities for XML honestly, objectively and effectively.

1 "Supervised Persons" means directors, officers, and partners of the Company (or other persons occupying a similar status or performing similar functions); employees of the Company; and any other person who provides advice on behalf of the Company and is subject to the Company's supervision and control.

While it is impossible to describe all of the possible circumstances under which a conflict of interest may arise, listed below are situations that most likely could result in a conflict of interest and that are prohibited under this Code of Ethics:

- Access persons may not favor the interest of one client over another client (e.g., larger accounts over smaller accounts, accounts compensated by performance fees over accounts not so compensated, accounts in which employees have made material personal investments, accounts of close friends or relatives of supervised persons). This kind of favoritism would constitute a breach of fiduciary duty; and

- Access persons are prohibited from using knowledge about pending or currently considered securities transactions for clients to profit personally, directly or indirectly, as a result of such transactions, including by purchasing or selling such securities.

- Access persons are prohibited from recommending, implementing or considering any securities transaction for a client without having disclosed any material beneficial ownership, business or personal relationship, or other material interest in the issuer or its affiliates, to the RCO. If the RCO deems the disclosed interest to present a material conflict, the investment personnel may not participate in any decision-making process regarding the securities of that issuer.

Access persons are prohibited from recommending, implementing or considering any securities transaction for a client without having disclosed any material beneficial ownership, business or personal relationship, or other material interest in the issuer or its affiliates, to the RCO. If the RCO deems the disclosed interest to present a material conflict, the investment personnel may not participate in any decision-making process regarding the securities of that issuer

Pursuant to paragraph 3.4.I of the Anti-Money Laundering and Combatting the Financing of Terrorism Handbook issued by the FSC in January 2020 and updated on 31 March 2021 (the "FSC Handbook"), the circumstances of the Company may be such that, due to the small number of employees, the Compliance Officer holds functions in addition to its functions of Compliance Officer as prescribed under Mauritius laws and regulations, or is responsible for other aspects of the Company's operations. Where this is the case, the Company must ensure that any conflicts of interest between the responsibilities of the Compliance Officer's role and those of any other functions are identified, documented and appropriately managed. The Compliance Officer however should be independent of the core operating activities of the Company and should not be engaged in soliciting business.

XML and its officers will act in the best interest of its clients.

- An interests register will be kept by the Company.
- The personal interests of a director, or persons closely associated with the director, must not take precedence over those of the Company and participants.

- A director should make his/her best effort to avoid conflicts of interest or situations where others might reasonably perceive there to be a conflict of interest.

- Full and timely disclosure, in writing, of any conflict, or potential conflict relating to directors and management must be made known to the Board.

- Where an actual or potential conflict does arise, on declaring their i nterest and ensuring that it is entered on the Register of interests of the Company, a director can participate in the debate and/or

indicate their vote on the matter, although such vote would not be counted. The director must give careful consideration in such circumstances to the potential consequences it may have for the Board and the Company.

- Directors should recognise that their duty and responsibility as director is always to act in the interests of the Company and not any other party.

- Directors and officers must treat confidential matters relating to the Company, learned in his/her capacity as director/ officer, as strictly confidential and must not divulge them to anyone without the authority of the Board. The Board must consider each such request on its merits and on a case by case basis.

Managing Conflicts of Interest

It is vital for XML which will be carrying out more than one regulated activity vis-a-vis Its clients, to identify and manage any con-flict of interest that may arise in the course of providing such services.

Conflict of interest may arise between XML's interest and that of its client and between the interests of one client and another, XML shall endeavour to manage these conflicts of interest by:

- Establishing well defined Chinese walls segregating the Management Functions and Advisory Functions
- Independent oversight
- Disclosure
- Declining to provide the service

A conflict of interest register shall be kept by each Committee. Any conflict of interest situations or potential conflicts situations should be reported immediately to the relevant Committee who shall escalate it to the Board XML.

Gifts and Entertainment

Supervised persons should not accept inappropriate gifts, favors, entertainment, special accommodations, or other things of material value that could influence their decision-making or make them feel beholden to a person or firm. Similarly, supervised persons should not offer gifts, favors, entertainment or other things of value that could be viewed as overly generous or aimed at influencing decision-making or making a client feel beholden to the Company or the supervised person.

No supervised person may receive any gift, service, or other thing of more than de minimis value from any person or entity that does business with or on behalf of the ID. No supervised person may give or offer any gift of more than de minimis value to existing clients, prospective clients, or any entity that does business with or on behalf of the ID without written pre-approval by the RCO. The annual receipt of gifts from the same source valued at $250.00 or less shall be considered de minimis. Additionally, the receipt of an occasional dinner, a ticket to a sporting event or the theater, or comparable entertainment also shall be considered to be of de minimis value if the person or entity providing the entertainment is present. All gifts, given and received, will be recorded in a log to be signed by the supervised person and the RCO and kept in the supervised persons file.

No supervised person may give or accept cash gifts or cash equivalents to or from a client, prospective client, or any entity that does business with or on behalf of the adviser.

Bribes and kickbacks are criminal acts, strictly prohibited by law. Supervised persons must not offer, give, solicit or receive any form of bribe or kickback.

Political and Charitable Contributions

Supervised persons that make political and charitable contributions, in cash or services, must report each such contribution to the RCO, who will compile and report thereon as required under relevant regulations. Supervised persons are prohibited from considering the ID's current or anticipated business relationships as a factor in soliciting political or charitable donations. This policy is only enforced if a government entity is a client of XML.

Confidentiality

Supervised persons shall respect the confidentiality of information acquired in the course of their work and shall not disclose such information, except when they are authorized or legally obliged to disclose the information. They may not use confidential informa-tion acquired in the course of their work for their personal advantage. Supervised persons must keep all information about clients (including former clients) in strict confidence, including the client's identity (unless the client consents), the client's financial circumstances, the client's security holdings, and advice furnished to the client by the Company.

Service on Board of Directors

Supervised persons shall not serve on the board of directors of publicly traded companies absent prior authorization by the RCO. Any such approval may only be made if it is determined that such board service will be consistent with the interests of the clients and of XML, and that such person serving as a director will be isolated from those making investment decisions with respect to such Company by appropriate procedures. A director of a private company may be required to resign, either immediately or at the end of the current term, if the Company goes public during his or her term as director.

Relationships with Regulatory Bodies

Officers may come into contact with representatives from regulatory bodies during the course of their work. Officers are expected to deal with the Regulators in a cooperative manner and must comply with any disclosure obligations in a prompt manner.

Compliance Procedures

Compliance with Laws and Regulations

All supervised persons of XML must comply with all applicable laws. Specifically, supervised persons are not permitted, in connec-tion with the purchase or sale, directly or indirectly, of a security held or to be acquired by a client:

- To defraud such client in any manner;
- To mislead such client, including making any statement that omits material facts;
- To engage in any act, practice or course of conduct which operates or would operate as a fraud or deceit upon such client;
- To engage in any manipulative practice with respect to such client; or
- To engage in any manipulative practice with respect to securities, including price manipulation

Personal Securities Transactions Procedures and Reporting

A. Pre-Clearance

All supervised persons must follow the following procedures before executing any personal trades.

I. Pre-clearance requests must be submitted by the requesting supervised person to the RCO or the appropriate supervisor in writ-ing. The request must describe in detail what is being requested and any relevant information about the proposed activity.

2. The RCO/supervisor will respond in writing to the request as quickly as is practical, either giving an approval or declination of the request, or requesting additional information for clarification.

3. Pre-clearance authorizations expire 48 hours after the approval, unless otherwise noted by the RCO on the written authorization response.

4. Records of all pre-clearance requests and responses will be maintained by the RCO for monitoring purposes and ensuring the Code of Ethics is followed.

B. Pre-Clearance Exemptions

The pre-clearance requirements of this section of this Code of Ethics shall not apply to:

I. Purchases or sales affected in any account over which the access person has no direct or indirect influence or control.

2. Purchases which are part of an automatic investment plan, including dividend reinvestment plans.

3. Purchases effected upon the exercise of rights issued by an issuer pro rota to all holders of a class of its securities, to the extent such rights were acquired from such issuer, and sales of rights so acquired.

4. Acquisition of covered securities through stock dividends, dividend reinvestments, stock splits, reverse stock splits, mergers, consolidations, spin-offs, and other similar corporate reorganizations or distributions generally applicable to all holders of the same class of securities.

5. Open end investment company shares other than shares of investment companies advised by the Company or its affiliates orsub-advised by the Company

6. Certain closed-end index funds.

7. Unit investment trusts.

8. Exchange traded funds that are based on a broad-based securities index.

9. Futures and options on currencies or on a broad-based securities index

C. Reporting Requirements

I. Holdings Reports

Every access person shall, no later than ten (10) days after the person becomes an access person and annually thereafter, file a holdings report containing the following information:

a. The title and number of shares of each Reportable Security in which the access person had any direct or indirect beneficial own-ership when the person becomes an access person;

b. The name of any broker, dealer or bank with whom the access person maintained an account in which any securities were held for the direct or indirect benefit of the access person; and

c. The date that the report is submitted by the access person.

2. Transaction Reports

Every access person shall, no later than ten (10) days after a security transaction is executed, file transaction reports containing the following information:

a. For each transaction involving a Reportable Security in which the access person had, or as a result of the transaction acquired, any direct or indirect beneficial ownership, the access person must provide the date of the transaction, the title and number of shares of each involved in the transaction;

b. The nature of the transaction (e.g., purchase, sale);

c. The price of the security at which the transaction was effected;

d. The name of any broker, dealer or bank with or through the transaction was effected; and

e. The date that the report is submitted by the access person.

3. Reporting Exemptions

The reporting requirements of this section of this Code of Ethics shall not apply to:

a. Any report with respect to securities over which the access person has no direct or indirect influence or control.

b. Transaction reports with respect to transactions effected pursuant to an automatic investment plan, including dividend reinvestment plans.

c. Transaction reports if the report would contain duplicate information contained in broker trade confirmations or account statements that the Company holds in its records so long as the Company receives the confirmations or statements no later than thirty (30) days after the end of the applicable calendar quarter.

d. Any transaction or holding report if the Company has only one access person, so long as the Company maintains records of the information otherwise required to be reported under the rule.

4. Report Confidentiality

All holdings and transaction reports will be held strictly confidential, except to the extent necessary to implement and enforce the provisions of the code or to comply with requests for information from government agencies

.

5. Risks and Complaints Officer Review of Personal Securities Information

The RCO or designated compliance officer will review all access person's personal securities transactions and holdings report after they have been collected. The officer will look to identify improper trades or trading patterns by access persons. All violations will be reported to the RCO.

Restricted Securities

XML does not maintain a list of restricted securities that supervised persons are restricted from trading in. XML requires all personal trades by members of the investment team to be precleared before executing. XML also requires a "portfolio first" rule. Any security that is being held, sold, or bought in XMLs portfolios, must be executed prior to any XML employee transaction.

Investing Personal Money in the Same Securities as Clients

From time to time, representatives of XML may buy or sell securities for themselves that is also in our portfolio. The RCO will always document any transactions that could be construed as conflicts of interest and XMl. will always transact client business before their own when similar securities are being bought or sold.

Certification of Compliance

Initial Certification

The Company is required to provide all supervised persons with a copy of this Code. All supervised persons are to certify in writing that they have: (a) received a copy of this Code; (b) read and understand all provisions of this Code, and (c) agreed to comply with the terms of this Code.

Acknowledgement of Amendments

The Company must provide supervised persons with any amendments to this Code and supervised persons must submit a written acknowledgement that they have received, read, and understood the amendments to this Code.

Annual Certification

All supervised persons must annually certify that they have read, understood, and complied with the Policies and Procedures and that the supervised person has made all of the reports required by this code and has not engaged in any prohibited conduct.

The RCO shall maintain records of these certifications of compliance.

Compliance Officer Duties

Training and Education

The RCO shall be responsible for training and educating supervised persons regarding this Code. Training will occur periodically as needed. All supervised persons are required to attend training sessions, read any applicable materials and acknowledge their training on the attestation provided in the Policies and Procedures manual.

Annual Review

The RCO shall review and test at least annually the adequacy of the Policies and Procedures and the effectiveness of its implementation. The RCO will attest that it has been reviewed and updated.

Email Review

The RCO will randomly review access person's emails once a quarter and document his/her review.

The Company must further keep record of:

- the identity and address of the client.
- if the customer is acting on behalf of another person:
- the identity and address of the person on whose behalf the customer is acting; and
- the customer's authority to act on behalf of that other person.
- if another person is acting on behalf of the client:
- the identity and address of that other person; and
- that other person's authority to act on behalf of the client.
- the nature of the business relationship or transaction.
- the intended purpose of the business relationship; and
- the source of funds which the prospective client is expected to use in concluding transactions in the course of the business relationship.

- in the case of a transaction:
    - the amount involved and the currency in which it was denominated.
    - the date on which the transaction was concluded;
    - the parties to the transaction.
    - the nature of the transaction; and
    - business correspondence.
    - if the Company provides account facilities, the identifying particulars of all accounts at the Company that are related to the transaction.
    - any document or copy of a document obtained by the Company in order to verify a person's identity. Further, the Company must keep records of:

    - All reports made to and by the MLRO/Deputy MLRO.
    - All training is provided in relation to AML and CFT.

Transactional records and or documents are kept at the registered office of the Company's Administrator's, IQ EQ Fund Services (Mauritius) Ltd, (the "**Administrator**"). Records should be sufficient to provide adequate evidence to the relevant local authorities to conduct their investigations.

Advertising Policy

The Company's RCO shall be responsible for approving all Company advertising and ensuring it is in compliance with jurisdictional regulations. No advertisement shall be distributed without the RCO's approval.

Compliance Requirements:

Pursuant to certain rules and regulations, an advertisement may not:

- Use or refer to testimonials (which include any statement of a client's experience or endorsement);
- Mislead clients using misrepresentations or exaggerations.
- Refer to past, specific recommendations made by the adviser that were profitable, unless the advertisement sets out a list of all recommendations made by the adviser within the preceding period of not less than one year, and complies with other, specified conditions.
- Represent that any graph, chart, formula, or other device can, in and of itself, be used to determine which securities to buy or sell, or when to buy or sell such securities, or can assist persons in making those decisions, unless the advertisement prominently dis-closes the limitations thereof and the difficulties regarding its use; and
- Represent that any report, analysis, or other service will be provided without charge unless the report, analysis or other service will be provided without any obligation whatsoever.

An advertisement shall include any notice, circular, letter, Email or other written communication (including any social media com-munications such as Facebook messaging, Twitter feeds, online biogs or any other internet communication) addressed to more than one person, or any notice or other announcement in any publication or by radio or television, which offers (1) any analysis, report, or publication concerning securities, or which is to be used in making any determination as to when to buy or sell any secu-rity, or which security to buy or sell, or (2) any graph, chart, formula, or other device to be used in making any determination as to when to buy or sell any security, or which security to buy or sell, or (3) any other investment advisory service with regard to securities.

Social Media Policy

The following websites are considered Social Media sites: 1) Facebook; 2) Twitter; 3) LinkedIn; 4) Instagram; 5) Reddit; 6) YouTube; 7) Biogs.

XML has adopted the following policies and procedures concerning the usage of social media websites by its supervised persons:

1) All social media site usage is considered correspondence and/or advertising by XML

2) All usage and posting to these sites must be monitored and approved by the Company's RCO

3) XML requires that all social media usage and posts must be retained and archived.

4) Supervised persons are not permitted to post any specific investment recommendations to social media

5) When investment recommendations place. discussed on any platform, there will be disclosures put in place

Accuracy of Disclosures Made to Clients, and Regulators

The RCO is responsible for the accuracy of all disclosures made to clients, and regulators. Where third party disclosure documents are involved, the RCO will verify that these documents are legitimate documents from the third party. XML will notify all clients re-ceiving these third-party documents that XML, has only verified the legitimacy and origin of the documents but has NOT verified or analyzed the information contained therein. The client will be instructed to conduct their own investigations to verify the informa-tion contained in each document including but not limited to a due diligence investigation.

Account Statements

XML will review client account statements to ensure their accuracy. All client account statements will be stored electronically, Cli-ents should refer to their custodial statements for an official record.

Advertisements

All advertisements are reviewed to ensure their accuracy, specifically in regard to any performance claims. The RCO will review all performance calculations contained in advertisements to ensure performance was accurately calculated.

Privacy Policy

The privacy policy statement is given to clients at the initial signing of the client contract and emailed once annually. A copy of the privacy policy is available on our website and can be provided at request.

Trading Policies

Best Execution Obligation

XML owes a fiduciary duty to clients to obtain best execution of their brokerage transactions. Failure by XML to fulfill its duty to cli-ents to obtain best execution may have significant regulatory consequences. XML's policies are modeled after the guidelines artic-ulated by the regulators; specifically, it believes that, to a significant degree, best execution is a qualitative concept. in deciding what constitutes best execution, the determinative factor is the lowest possible commission cost, whether the transaction rep-resents the best qualitative execution. In making this determination, XML's policy is to consider the full range of the broker's ser-vices, including without limitation the value of research provided, execution capabilities, commission rate, financial responsibility, administrative resources and responsiveness.

Execution by brokers: All trades are electronic, fully regulated and transparent.

Trade Errors

A trade error occurs when there is a deviation from the general trading practices involving transactions and settlements of trades for a client's account. Part of XML's fiduciary obligation is to identify and correct these errors as soon as discovered. It has been accepted in the industry to recognize the following as trade errors:

l. A sell is executed as a buy.

2. The over/under allocation of a security i.e., a comma is placed in the wrong place or an additional O is added (1,000 turns into 10,000).

3. An incorrect ticket symbol (c instead of s)

4. Trade takes place in an incorrect account number.

5. A purchase or sale order fails to be executed.

6. Limit order is executed at market price.

7. Block trades are allocated inaccurately.

8. Client account does not have the funds to settle the transaction.

9. The purchase or sale of securities is transacted in violation of the client's investment profile or guidelines.

10. The purchase or sale of securities for non-discretionary clients are executed prior to or without receiving client consent, or with-out proper documented authorization.

The following types of errors will not be deemed to be a trade error as defined by your RIA:

l. An incorrect trade that was caught prior to settlement thereby not having a negative impact on your client.

2. A trade that was improperly documented.
3. The rewriting of tickets that describe or correct improperly executed transactions.
4. Errors that are made by unaffiliated third parties (broker/dealer, custodian, etc.). as a fiduciary, the Company is responsible to review the trades and ensure that third party errors are favorably resolved.

XML's policy is to ensure that clients are never responsible for a trade error. If XML is responsible for the error, it will correct the error the same day if possible. If a third party is responsible, XML will oversee the resolution. Any loss will be reimbursed to the client in the form of a statement credit or check written by XML, if the custodian or broker/dealer does not cover it under the de minimis.

All trade errors must be timely addressed to the RCO once discovered. The RCO should document when the trade error and wheth-er XML is responsible. If responsible, XML must then look to correct the error immediately, following fiduciary standards acting in the client's best interest. Any client losses must be reimbursed by XML for the full amount of the loss, including the reimbursement of the transaction fees. If there is a profit resulting from the error:

l. XML may elect to allow the client to retain the profit.

2. The custodian of broker/dealer may retain the profit; or

3. It is best practice to hold the profits in a Company trade error account in accordance with XML'S accounting standards and donated to charity annually.

All payments made to clients will be properly documented.

Trade Error File

XML will maintain a trade error log. All trade errors will be properly documented and maintained by the RCO.

Portfolio Management Processes

XML provides discretionary account management on a continuous basis. XML invests in public equities, cash and other securities that are deemed suitable, governed by the investment management agreements in place.

Research Processes

The investment team utilizes information obtained from a wide variety of sources. Increasingly, the Internet and new databases provide a wealth of ideas and information to enhance XML's research.

Industry research is used to supplement XML's own research efforts. XML employees research investments on a daily basis. Exam-ples of on-line resources include financial news websites, and Reuters.

Information Security &. Cybersecurity

XML has taken extensive measures to safeguard the privacy and integrity of the information that it gathers, stores, and archives during its normal business practices. Computer security measures have been instituted where applicable including passwords, backups, and encryption. All employees are informed and instructed on various security measures including the non-discussion and/or sharing of client information, always removing client files from desktops or working areas that cannot be locked or secured, and proper storage of client securities files in locked files or other secured location. XML maintains physical, electronic, and proce-dural safeguards to guard nonpublic personal information.

In addition to electronic and personnel measures, XML has implemented reasonable physical security measures at our office loca-tions to prevent unauthorized access to our facilities.

Third Party Vendors

XML uses various methods to store and archive client files and other information. All third-party services or contractors used have been made aware of the importance XML places on both Company and client information security.

XML utilizes various third-party vendors for its business activities. XML has collected, reviewed and maintains the privacy policies and cybersecurity policies of all its third-party vendors.

Cybersecurity Risks and Controls

XML periodically assess the nature, sensitivity and location of information it collects and maintains. As a financial institution, XML understands our business is vulnerable to cybersecurity incidents. XML has put tools in place tomitigate these risks including but not limited to: anti-virus software, firewalls, VPNs, and using unique passwords on computers, documents and third-party technol-ogy systems used.

XML recognizes that employee's emails are susceptible to potential hacks or malicious phishing attempts. To avoid these events, all employees are required to use 2-factor authentication for email logins.

XML utilizes a cloud-based drive that is backed-up daily and monitored to prevent data loss.

Access Control Policy

XML employees are limited to viewing and sharing files on both internal and third-party systems that are only relevant to their roles. Upon termination of an employee, there will be an immediate termination of access. rights to all systems and offices.

Mobile Device Security

XML employees utilize their personal mobile phone devices for e-mail management while away from their main offices. XML em-ployees are required to have 2-step authorization on their email accounts and should only log in to their email on a trusted device. Employees are encouraged to enable passwords on their mobile devices. Employees are instructed to use the Company's VPN, which is mandated while traveling and using public Wi-Fi.

If employees misplace their mobile devices, they should communicate this to the RCO immediately so their email account can be disassociated with their device.

Employee Training

XML employees are periodically trained on cybersecurity risks and the tools they can utilize to keep our information safe. Common employee related cybersecurity issues include improper protection of a Company computer or mobile device, poor password management, not utilizing two-factor authentication, the inability to recognize email phishing attacks or using outdated anti-virus software. Employees are made aware of the cybersecurity threats made towards our organization and are taught to be vigilant.

Malicious actors may try to pose as XML, clients and attempt to wire proceeds to their accounts. To avoid this happening, employ-ees will verbally confirm all wire requests with the phone number we have on file for such client.

In the event of a cybersecurity breach, the RCO will notify all employees and instruct them to change all passwords. The RCO will notify all clients of the nature of the event and how we are working to remediate the situation. XML will work with its third-party se-curity vendors to resolve the security issue.

Incident Response

In the event of a cybersecurity issue, the RCO will take immediate action to rectify the situation. If related to an employee's email, the e-mail account will be inactivated and follow the procedures created to notify all parties involved. The RCO will scan the net-work for any data loss, email hacking and will notify all employees to scan their anti-virus software. If any vendors or clients are in-volved, the RCO will alert them as soon as possible and instruct them to delete any suspicious emails.

XML has enabled automatic email alerts that are sent to the RCO and CEO if Google detects any phishing scams, suspicious logins, or any other cybersecurity incidents. The RCO will document all incidents and their remediation efforts. XML employees have en-abled two-factor authentication on their email accounts to reduce the likelihood of such attempts.

Financial Resources

Relevant officers should ensure that XML always maintains adequate financial resources to meet its financial obligations and is able to withstand the risks to which XML is subject to. In light of the above, the Company can observe the following:

- Conducting a solvency test as required under Section 6 of the Mauritius Companies Act 2001 (the "**Companies Act**") prior to distributing funds to its shareholders.

- A letter of support can be requested from the Shareholders to ensure that the financial obligations of the Company can be met.

- To ensure that audited financial statements of the Company are prepared and submitted to the FS within the requisite deadlines.

Protection of Customer's/Company's Assets

Where an officer has control of or is otherwise responsible for assets belonging to the Company which the Company is required to safeguard, he should arrange proper protection for them, by way of segregation and identification of those assets. Officers must not engage in fraudulent or any other dishonest activity involving the property or assets of XML.

All of XML's property and assets must not be considered as the officer's personal property. They should only be used for the benefit of XML. An officer must act with utmost care and diligence to ensure that XML's customers' funds are not commingled with the Company's own funds or those of its affiliates or funds belonging to other customers. XML generates, receives and stores informa-tion from various sources. Officers have the responsibility to ensure that such information to which they have access or under their control are properly safeguarded Officers must not make any false and/or artificial entries in the books and records of XML for any reason.

Officers should not disclose XML's customers' confidential information or allow such disclosure, unless prior authorization has been obtained from the relevant customers. This obligation continues beyond the termination of the officer's employment with XML. Offi-cers must use their best efforts to avoid unintentional disclosure of confidential information by adhering to existing processes within XML and applying special care when storing or transmitting confidential information.

Fit and Proper Standards for XML

Competence and Capability

To assess the competence and capability of its officers, XML will ensure that they act in a knowledgeable, professional and efficient manner by complying with the requirements of the applicable laws. XML will appoint officers who have:

- appropriate range of skills and experience.
- technical knowledge and ability to perform the prescribed duties for which they will be engaged, especially with recognized professional qualifications and membership of relevant professional institutions.
- relevant satisfactory past performance or expertise.

Honesty, integrity and fairness

In determining the honesty, integrity and reputation of the person which the Company intends to engage, XML will consider wheth-er the person has been convicted of offences such as fraud, dishonesty, money laundering, terrorist financing, theft, or other finan-cial crimes.

Financial soundness or Insolvency

XML will ensure the financial soundness of the Company by imposing adequate control over financial risks on a continuing basis.

The Company's RCO shall be responsible for handling complaint reviews.

- All clients' complaints against XML shall be directed to [complaints@xtreamforex.com]
- Receipt of complaints shall be acknowledged by the Company and be dealt with within thirty (30) days.
- All complaints shall be taken seriously, handled transparently and promptly investigated. The RCO shall ensure that all complaints be dealt with in an independent courteous and efficient manner and resolved within the delay as stated in paragraph above.
- The Company shall maintain complaints register (the "Complaints Register") to record all complaints received. The record shall include the date on which the complaint has been made, date acknowledged, category of complaints and actions taken.
- No complaint should be left unresolved and the date the complaint is "closed" should be noted on the complaint filing.

Anti-Money Laundering and Combatting Financing of Terrorism (AML/CFT)

The Board of the Company has adopted an AML/CFT Framework to combat money laundering and financing of terrorism as per the requirements of the FIAMLA, FIAMLR 2018, the FSC Handbook and other relevant guidelines/circulars issued by the FSC.

The Board has put the following into operation:

- programs for assessing risk relating to money laundering and financing of terrorism.
- the formulation of a control policy that will cover issues of timing, degree of control, areas to be controlled, responsibilities and follow-up.
- monitoring programs in relation to complex, unusual or large transactions.
- enhanced due diligence procedures with respect to persons and business relations and transactions carrying high risk, and high-risk countries in accordance with section 17H of the FIAMLA, and wit persons established in jurisdictions that do not have adequate systems in place against money laundering and financing of terrorism;
- providing employees, including the Money Laundering Reporting Officer, from time to time with training in the recognition and handling of suspicious transactions.
- making employees aware of the procedures under the FIAMLR 2018, the FSC Handbook and any other relevant policies, guidelines/circulars; and
- establishing and maintaining a manual of compliance procedures in relation to anti-money laundering.

The Board should ensure compliance with the requirements of FIAMLA and FIAMLR 2018 and the following forms part of the AML/CFT framework adopted by the Company:

(i) The Board is responsible for managing the Company effectively and is in the best position to understand and evaluate all po-tential risks to the financial institution, including those of money laundering and financing of terrorism. The Board must therefore take ownership of, and responsibility for, the business risk assessments and ensure that they remain up to date and relevant. On the basis of its business risk assessment, the Board must establish a formal

strategy to counter money laundering and financing of terrorism. Where the Company forms part of a group operating outside Mauritius, that strategy may protect both its global reputation and its Mauritius business. The Board must document its systems and controls (including policies and procedures) and clearly apportion responsibilities for countering money laundering and fi-nancing of terrorism, and, in particular, responsibilities of the Compliance Officer ("CO") and Money Laundering Reporting Officer **("MLRO")**

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

(iii) The Board must consider the appropriateness and effectiveness of its compliance arrangements and its policy for the review of compliance at a minimum annually, whenever material changes to the Company occur. Where, as a result of its review, chang-es to the compliance arrangements or review policy are required, the Board must ensure that the Company makes those changes in a timely manner.

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

(vi) The Board must document its systems and controls (including policies and procedures) and clearly apportion responsibilities for the money laundering and financing of terrorism, and, in particular, responsibilities of the MLRO and CO.

(vii) According to the FSC Handbook, the board or senior management of the Company must establish documented systems and controls which:

a) undertake risk assessments of its business and its customers.

b) determine the true identity of customers and any beneficial owners and controllers.

c) determine the nature of the business that the customer expects to conduct and the commercial rationale for the business relationship.

d) require identification information to be accurate and relevant.

e) require business relationships and transactions to be effectively monitored on an ongoing basis with particular attention to transactions which are complex, both large and unusual, or an unusual pattern of transactions which have no apparent economic or lawful purpose.

f) compare expected activity of a customer against actual activity.

g) apply increased vigilance to transactions and relationships posing higher risks of money laundering and financing of terrorism.

h) ensure adequate resources are given to the CO to enable the standards within the FSC Handbook to be adequately implemented and periodically monitored and tested.

i) ensure procedures are established and maintained which allow the MLRO and the Deputy MLRO to have access to all relevant information, which may be of assistance to them in considering suspicious transaction reports ("STRs");

Prevention of Money Laundering and Terrorist Financing

The legislative framework has been set by the FIAMLA, followed by the FIAMLR 2018 which are effective since 01 October 2018

In April 2012, the Code on Prevention of Money Laundering and Terrorist Financing issued by FSC in 2012 (the "FSC Code") came into effect and the same was updated on 25 May 2017. However, the FSC has, on 06 November 2020, by way of a Circular Letter refer-enced as CL061120, repealed the FSC Code until the issuance of any additional enforceable Anti Money Laundering/Combatting Terrorist Financing (AML/CFT) requirements.

However, the repeal of the FSC Code will not, inter alia, affect any obligations or liability incurred thereunder, nor will it affect any-thing done or suffered under the repealed FSC Code

The FSC has reserved itself the right to take any regulatory or disciplinary actions for any breaches of the said code which have occurred on or before the 06 November 2020.

In addition, the FSC issued its new FSC Handbook on 13 January 2020 to provide guidance to financial institutions on the anti-mon-ey laundering, financing of terrorism and financing of proliferation of weapons of mass destruction framework. The FSC Handbook is a supplement to the FSC Code. Although the FSC Handbook does not aim to prescribe an exhaustive list of recommended AM-L/CFT practices, it shall assist financial institutions in shaping their systems of internal controls on areas such as risk-based ap-proach, customer due diligence measures, electronic identification and verification, monitoring of transactions whether automated or manually, screening and training of staff, to name a few. The FSC would take the FSC Handbook guidance into account when as-sessing the level of compliance with the FIAMLA and FIAMLR 2018 while conducting onsite visits.

The Company is required under its GBL to adopt, enforce and re-assess on an annual basis, its anti-money laundering and com-bating of financing of terrorism framework.

Money Laundering

Definition

The goal of a large number of criminal acts is to generate a profit for the individual or group that carries out the act. Money laun-dering is the processing of these criminal proceeds to disguise their illegal origin. This process is of critical importance, as it en-ables the criminal to enjoy these profits without jeopardizing their source. Illegal arms sales, smuggling, and the activities of orga-nized crime, including for example drug trafficking and prostitution rings, can generate huge amounts of proceeds. Embezzlement, insider trading, bribery and computer fraud schemes can also produce large profits and create the incentive to "legitimize" the ill-gotten gains through money laundering.

Put simply, money laundering involves the channeling of proceeds of illegal activity into the stream of commerce and finance in order to disguise the nature, location, source, ownership or control of such proceeds.

Money Laundering Cycle

Money laundering is not a single act but is in fact a process that is accomplished in basic steps. These steps can be taken at the same time in the course of a single transaction, but they can also appear in separable forms one by one as well. The steps are: -

(i) Placement

This is the first stage in the washing cycle or the initial point of entry of "dirty money" into the legitimate financial system. This can be done by breaking large amounts of cash into less conspicuous, smaller amounts that are then deposited into a bank ac-count.order to disguise the nature, location, source, ownership or control of such proceeds.

(ii) Structuring/Layering

This is the deliberate creation of complex transactions to hide the criminal origin of the money. It is typically designed to confuse the law enforcement who would be forced to commit more resources to follow a more complex paper trail. The laundered might simply wire funds through a series of accounts.

(iii) Integration

This is the ultimate introduction of money into the legitimate financial system where the criminal believes it would no longer be possible or easy to associate with the underlying criminal offence.

Policy

In view of the above, summarized below is the Company's "Anti-Money Laundering Policy" based on the provisions contained in the Mauritius AML laws and applicable regulations, and guidelines issued by the FSC in this regard.

The Company shall not accept funds in cash or third-party cheques from clients. It is the policy of the Company to seek to prevent the misuse of the funds it manages, as well as preventing the use of its personnel and facilities for the purpose of money launder-ing and terrorist financing. The Company has adopted and enforces policies, procedures and controls with the objective of detect-ing and deterring the occurrence of money laundering, terrorist financing and other illegal activity.

Anti-money laundering ("AML") compliance is the responsibility of every employee (as applicable). Therefore, any employee (as applicable) detecting any suspicious activity is required to immediately report such activity to the MLRO/ DMLRO under the FIAMLR 2018. The employee (as applicable) making such a report should not discuss the suspicious activity or the report with the client in question or with any other person that may jeopardize further investigation of the matter by law enforcement authorities

The MLRO is responsible for ensuring that the Company complies with the applicable AML laws and regulations.

The MLRO/DMLRO will review any reports of suspicious activity which have been observed and reported by employees (as applica-ble) and report to the FIU where appropriate.

Client Acceptance Policy and Procedures

All person's sourcing clients on behalf of the Company shall be required to adhere to the requirements specified herein below that are aimed to identify the types of clients that are likely to pose a higher than the average risk of money laundering or terrorist fi-nancing.

The Client Acceptance Policy and Procedures adopted by the Company can be found in the AML/ CFT Framework adopted by the Company.

Screening

Screening covers Sanction, PEPs and Adverse Media on the customers, Associated Parties, beneficial owners ("BO") and all parties identified in the organizational and control structure. The Company shall ensure that its customers, connected parties of custom-ers and all natural persons appointed to act on behalf of customers are screened through World Check and Internet Check for the purpose of determining if there are any money laundering and terrorism financing risks in relation to the customers.

All new customers and their Associated Parties (including B.O., Immediate, Intermediate and Ultimate owners) must be screened up front through World Check and Internet Check, prior to on boarding. Existing customers must also be screened continuously. It is the Company's responsibility to ensure that ongoing screening is carried out on its applicants for business.

The PEP Policy adopted by the Company can be found in the AML/CFT Framework adopted by the Company.

Sanctions Screening

Sanctions are measures imposed by governments across the world in response to a variety of international issues including terror-ism and nuclear weapons proliferation. Sanctions make it an offence to do business with persons or entities listed in such sanc-tions and in some cases, the assets of sanctioned individuals/entities are subject to an asset freeze. Sanctions lists are localand-/or international lists of persons and entities with whom a business relationship may not be established and their assets, where applicable, are to be frozen.

These lists include the Office of Foreign Assets Control (OFAC), United Nations Security Council (UNSC) and European Union (EU) which are incorporated into the World Check Compliance screening performed by the Company.

Sanctions screening of all cus-tomers and where possible suppliers against applicable local and international sanctions and PEP lists shall be conducted.

Where sanctions screening identifies a potential match, the result must be properly investigated in order to determine whether it is a positive match. In the event that the match is positive, it must be reported to the CO for further investigation.

The Targeted Financial Sanctions Policy adopted by the Company can be found in the AML/ CFT Framework adopted by the Company.

Ongoing monitoring for PEP

Once a business relationship has been established with a PEP, on-going monitoring must be conducted on all related transactions to ensure that they are in line with the customer's source of funds and wealth and original account mandate. This can be achieved by requesting for additional information to understand the purpose of a transaction and verifying the provenance of the source of funds and where required, to request for evidentiary documents such as agreements, invoices, bank statements, etc.

Furthermore, quarterly World Check and Internet Check must be conducted on the PEP and evidence of such screening kept on re-cords.

Annual reviews must be conducted on all customers identified as PEPs and approved by Board / Senior Management.

The following information and documentation must be reviewed/reconfirmed/updated when conducting an annual review of a PEP investor:

- all KYC information.
- the relevance of the EDD conducted initially including reconfirmation of the customer's source of funds and source of wealth; and
- where adverse information such as ongoing litigation or regulatory proceedings were noted as part of the on-boarding information, further checks must be undertaken to ascertain any outcomes or obtain updated information.

Information obtained from the customer may be compared against additional independent sources in order to verify the accuracy of the information. The formal decision and reasons to either maintain or terminate the PEP relationship must be documented.

Factors to consider in establishing/maintaining/terminating a customer relationship with a PEP.

The following are factors, which should be considered in deciding whether to establish/ maintain/terminate a customer relation-ship with a PEP:

- funding of the account are the Company's in the account in line with the customer's source of funds and wealth and original account mandate;
- is there a history of suspicious or unexplained transactions.
- is the customer responsive to requests for up-to-date information.

There should be a detailed consideration of the rationale for establishing, maintaining, or terminating the business relationship with the PEP

[Note - where a customer has been accepted and the said customer or its beneficial owner or its associate or its family member is subsequently found to be, or subsequently becomes a PEP, appropriate EDD and Company Board's approval should be obtained as per above in order to continue such business relationships.]

Connected persons that are PEPs.

'Connected persons will include underlying principals such as beneficial owners and controllers.

The Company must apply appropriate EDD measures on a risk-sensitive basis where an applicant for business or customer (or any connected person, such as a beneficial owner or controller) is a PEP, and must ensure that they operate adequate policies, proce-dures and controls to comply with this requirement.

The Company must:

(a) develop and document a clear policy on the acceptance of business relationships or one-off transactions with such persons and ensure that this is adequately communicated.

(b) obtain and document the approval of senior management prior to establishing relationships with such persons.

(c) where such persons are discovered to be so only after a relationship has commenced, thoroughly review the relationship and obtain senior management approval for its continuance; and

(d) apply EDD measures to establish the source of funds and source of wealth of such persons.

Targeted Financial Sanctions

In order to ensure that employees (if applicable) are of the required standard of competence, which will depend on the role of the employee, the Company gives consideration to screening the employees against the UN's list of designated persons under terrorist and proliferation financing targeted financial sanctions, prior to, or at the time of, recruitment.

The Company also carries out periodic ongoing of its employees against the UN's list of designated persons under terrorist and proliferation financing targeted financial sanctions.

Section 23(1) of the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 (the "UN Act") pro-vides that subject to the said Act, no person shall deal with the funds or other assets of a designated party or listed party, includ-ing -

a) all funds or other assets that are owned or controlled by the designated party or listed party, and not just those that can be tied to -

i) a particular terrorist act, plot or threat.

ii) a particular act, plot or threat of proliferation

b) those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by the designated party or listed party.

c) funds or other assets derived or generated from funds or other assets owned or controlled, directly or indirectly, by the desig-nated party of listed party, and

d) funds or other assets of a party acting on behalf of, or at the direction of, the designated party or listed party.

In addition, section 23(2) of the UN Act provides that where a prohibition is in force, nothing shall prevent any interest which may accrue, or other earnings due, on the accounts held by a listed party, or payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the prohibition, provided that any such interest, earnings and payments continue to be subject to the prohibition.

Where a party is listed pursuant to UNSCR 1737 and the listing continues pursuant to UNSCR 2231, or is listed pursuant to UNSCR 2231, the National Sanctions Committee may authorize the listed party to make any payment due under a contract, an agreement, or an obligation, provided that the National Sanctions Committee:

a) is satisfied that the contract, agreement, or obligation was entered prior to the listing of such party.

b) is satisfied that the contract, agreement, or obligation is not related to any of the prohibited items, or services referred to in UNSCR 2231 and any future successor resolutions.

c) is satisfied that the payment is not directly or indirectly received from, or made to, a person or entity.

d) subject to the measures in paragraph 6 of Annex B to UNSCR 2231; and

e) has, lO working days prior to such authorization, notified the United Nations Sanctions Committee of its intention to authorize such payment.

In addition, any person who holds, controls, or has in his custody or possession any funds or other assets of a designated party or listed party shall immediately notify the National Sanctions Secretariat of -

a) details of the funds or other assets against which action was taken in accordance with subsection (1).

b) the name and address of the designated party or listed party.

c) details of any attempted transaction involving the funds or other assets, including -

d) the name and address of the sender.

e) the name and address of the intended recipient.

f) the purpose of the attempted transaction.

g) the origin of the funds or other assets; and

h) where the funds or other assets were intended to be sent.

Any person who fails to comply with Section 23 (1) or (2) 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 imprison-ment for a term of not less than 3 years.

Section 24(1) of the UN Act relating to prohibition on making funds or other assets available to designated party or listed party available, provides that subject to the UN Act, no person shall make any funds or other assets or financial or other related services available, directly, or indirectly, or wholly or jointly, to or for the benefit of -

a) a designated party or listed party.

b) a party acting on behalf, or at the direction, of a designated party or listed party; or

c) an entity owned or controlled, directly or indirectly, by a designated party or listed party.

The Economic Sanctions Policy adopted by the Company can be found in the AML/ CFT Framework adopted by the Company.

Adverse Media - Determining the level of significance of information.

The following should be considered when determining the level of significance of any information identified as a result of adverse media searches:

- Date of occurrence: The date of occurrence should be considered as the most recent date associated with the event/ activity, as opposed to the first time it was reported. E.g., where the adverse media relates to alleged events, the date of the latest investiga-tion or allegation should be used; where an offence has been confirmed, the date of conviction should be used. Although the length of time since an event occurred may not ultimately alter its significance, more recent events should be treated with additional caution, particularly in the case of alleged events as there may be less information available to validate the legitimacy of the event.

- Note: 'recent' means between 12 months to 5 years depending on the nature, severity and penalty of the alleged/ confirmed offence.

- The nature of the allegation/fact: The full nature of the allegation, including any criminal or civil indictments should be recorded. It should be noted whether the allegation relates to money laundering or terrorist financing or potentially could result in money laundering or terrorist financing.

- Whether the information is an allegation or fact: Consider whether the information identified is alleged, e.g., rumors, arrests but no charges brought, or whether actual involvement has been confirmed, e.g.,through convictions or fines.

- Reliability of the source of the information: Identify and record each source consulted for information obtained.

Verification of source of funds and source of wealth

The source of funds and source of wealth are required to be verified to demonstrate a thorough understanding of the source of the initial and ongoing funds and wealth that will pass through the customer's account/product held at the Company. Where initial funding is provided by third parties, the Company should ensure that the relationship between the parties is fully documented and a rationale for such a relationship is recorded and analyzed. If there is no proven rationale for the existence of such a relationship, further due diligence must be conducted and if required, escalated to Compliance for further investigation.

The source of funds and source of wealth of the PEP must be verified in accordance with the source of funds and source of wealth requirements applicable to that PEP.

Control Systems

To assist in the proper monitoring and control of suspicious transactions, the Board should set up a control system by appointing a Compliance Officer who shall have a direct reporting line to the Board. The latter will report to the Board on a quarterly basis on issues relating to money laundering and other related subjects including external laws, rules, codes, regulations.

Transaction Examination

Reasonable steps would be taken to allow the identification of suspicious transactions. In the recognition of suspicious transac-tions, employees should be particularly aware of two essential elements:

(a) the usual nature of the client's business (Know Your Client - KYC); and

(b) the usual type of business carried out by the Company (Know Your Business - KYB) principles. Suspicion should be aroused where the two principles do not match. Employees should report all transactions that they suspect to be linked to criminal activity. They are not allowed to turn a blind eye to the transaction as it might amount to an offence under the FIAMLA.

Appointment of Compliance Officer (co), Money Laundering Reporting Officer (MLRO) and Deputy MLRO (DMLRO)

Compliance Officer

Regulations 22 (1) of the FIAMLR 2018, requires that the Company designates a CO at senior management level for undertaking the day-to-day oversight of the AML Program for combating anti-money laundering and terrorism financing.

Currently, Mr. Kishen Kumar Hurhinidee has been appointed as the Company's CO and as per Regulation 22(3) of FIAMLR 2018, his responsibilities will entail the following:

(i) ensuring continued compliance with the requirements of the FIAMLA and FIAML Regulations 2018 subject to the ongoing over-sight of the Board of the Company.

(ii) undertaking day-to-day oversight of the AML Program

(iii) regular reporting, including reporting of non-compliance to the Board of the Company; and

(iv) contributing to designing, implementing, and maintaining the Company's compliance manual, policies and procedures and system for combating ML/TF.

MLRO/ DMLRO

Further, Regulation 26 of the FIAMLR 2018 requires the Company to appoint a MLRO and a DMLRO to whom all internal reports of suspicious transactions must be made.

In that respect, Mr Sandev Singh Soobagrah has been appointed to act as the MLRO and Mr. Kishen Kumar Hurhinidee as the DMLRO.

According to Regulation 26(4) of the FIAMLR 2018, the MLRO and DMLRO must be:

(a) be sufficiently senior in the organization of the financial institution or have sufficient experience and authority; and

(b) have a right of direct access to the board of directors of the financial institution and have sufficient time and resources to efectively discharge his functions.

The MLRO/ DMLRO is the person who is nominated to ultimately receive internal disclosures and who considers any report to deter-mine whether an external disclosure is required.

The responsibilities of the MLRO will normally include, as stated in the FIAMLR 2018:

- undertaking a review of all internal disclosures in the light of all available relevant information and determining whether or not such internal disclosures have substance and require an external disclosure to be made to the FIU.
- maintaining all related records.
- giving guidance on how to avoid tipping off the customer if any disclosure is made.
- liaising 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; and providing reports and other information to senior management.

The MLRO shall provide a quarterly report on the above to the Board and the Company is required under its FSC licence to re-as-sess on an annual basis its anti-money laundering and combating financing of terrorism framework.

In the absence of the MLRO, the DMLRO is expected to fulfill the duties described above. The DMLRO should be of similar status and experience to the MLRO.

Hiring of Employees and Employees' Training

The Company shall have adequate screening procedures in place to ensure high standards when hiring employees (as applica-ble). They shall identify the key positions within their own organization structures having regard to the risk of money laundering and terrorist financing and the size of their business and ensure the employees (as applicable) taking up such key positions are suitable and competent to perform their duties.

Regulation 22(1)(c) of FIAMLR 2018 states that the programmes for money laundering and terrorist financing should also cater for ongoing training programmes for the directors, officers and employees (as applicable) of the Company. Unless regulatory devel-opments dictate more frequent updates, the Company's staff will be updated annually on AML regulatory changes and develop-ments. However, the Company recognizes that some categories of employees (as applicable) should receive additional, special-ized training according to their roles within the Company.

One of the key components of an effective Compliance Program is employee training. At minimum, training must include:

Explanation of the Company's policies and procedures

- Guidance on how to identify suspicious activity and structured transactions.
- Procedures for verifying customer identity.
- Familiarity with required forms
- Recordkeeping and reporting requirements

Section 12.8.2 of the FSC Handbook further provides for ongoing professional development of the MLRO/DMLRO since the latter has significant responsibility for the receipt, evaluation, and where appropriate external reporting of suspicious transactions to the FIU.

Training will encompass familiarizing himself/herself with:

- AML/CFT legislative and regulatory requirements.
- FATF 40 Recommendations and reports on ML/TF typologies that examine trends in money laundering activity.

the identification and management of ML/TF risk.

- the design and implementation of internal systems of AML/CFT control.
- the design and implementation of AML/CFT compliance testing and monitoring programs; and
- the identification and handling of suspicious activity and arrangements and suspicious attempted activity and arrangements.

The designated CO will also receive in-depth training on all aspects of the prevention and detection of ML/TF.

The Board and senior management must receive adequate training to ensure they have the knowledge to assess the adequacy and effectiveness of d, procedures, and controls to counter the risk of ML/TF.

The FSC Handbook states that training will need to be conducted in light of new legislation or changes to the FSC Handbook or with the introduction of new products, services or practices.

Client Identification and Verification

In order to comply with Regulation 3(1) of the FIAMLR 2018, the Company has established procedures to ensure that all clients' identities have been verified on a risk-based approach before an account is opened or an investment is made into any private funds or limited partnerships managed by the Company.

Before opening an account for the clients, the Company will collect satisfactory documentary evidence required under the appli-cable provisions of the FIAMLR 2018 made thereunder.

In the event where clients are introduced to the Company by 'introducers', a form of third-party reliance, the Company has the ob-ligation to subject such third-party introducers to the full identification and verification CDD measures as provided under Regula-tions 3(a), (c) and (d) of the FIAMLR 2018.

Prohibited clients.

The Company will not open accounts or accept funds or securities from, or on behalf of, any person or entity whose name appears on the List of Specially Designated Nationals and Blocked Persons maintained by the United States Office of Foreign Assets Control, UN and EU list of sanctioned entities, from any Foreign Shell Bank or from any other prohibited persons or entities, as may be man-dated by the applicable law or regulation of the jurisdiction where the Company operates.

The Company will also not accept High-Risk clients (with respect to money laundering or terrorist financing) without conducting enhanced, well-documented due diligence regarding such prospective client.

With respect to separately managed client accounts and investors in private funds sponsored by the Company and other clients of the Company, the CO or the designated officer shall check the Office of Foreign Asset Control (OFAC), Worldcheck, United Nations Security Council list (1988 List, Al-Qaida sanction list), i nvestor alerts and warnings from international bodies such as !OSCO or such other lists as may be appropriate to ascertain whether investors and clients (and their principals) are posted there. The sub-scription documents for each private fund also require anti-money laundering representations by each investor, including that such investor is not a prohibited investor (as set forth therein). The subscription documents permit the private fund to freeze an investor's investment, if it reasonably believes that the investor is a prohibited investor or has otherwise breached its representa-tions.

Cash Transaction Reports

Section 5 of the FIAMLA stipulates that any person who makes or accepts any payment in cash in excess of 500,000 rupees or an equivalent amount in foreign currency, or such amount as may be prescribed, shall commit an offence.

As it is, the Company or its private funds do not accept subscriptions in cash and only accepts funds that are wired into the bank account of the Fund. If any employee (as applicable) were to receive cash from any client or prospect, such employee (as appli-cable) should contact the CO and the MLRO immediately.

Company Administrator

The Company has entered into an administration agreement with the appointed Administrator, which will act as the Administrator of the Company. The Administrator must be licensed with the FSC as a Management Company and supervised by the FSC in terms of its AML/CFT controls.

The Administrator will perform:

- Certain administrative functions.
- Accounting.
- Registrar.
- Transfer agency services for the Company (e.g., Customer/ Shareholder register); and
- Transactional record keeping

Where the Administrator outsources certain of its functions to an Administrator Agent, the Administrator enters into an administra-tion agreement with the Administrator Agent, however, the approval for the use of the Administrator Agent to conduct functions of the Administrator must be approved and vetted by the Board first.

Outsourcing of compliance-related functions

The Company may outsource some or all of its compliance functions related to AML/ CFT to a third party which shall ensure that the Company implements its program for combating money laundering and terrorism financing and managed all potential risks relating thereto in accordance with its own policies and procedures.

Prior to outsourcing the compliance-related functions, the Company shall assess the policies and processes of the third party.

Risk Based Approach

Aims of adopting a risk-based approach

A risk-based approach towards the prevention and detection of ML and TF aims to support the development of preventative and mitigating measures that are commensurate with the ML and TF risks identified by the financial institution. This approach also aims to deal with those risks in the most cost-effective and proportionate way.

Section 17 of the FIAMLA provides for a duty for the financial institution to identify, assess and understand its money laundering and terrorism financing risks. Furthermore, section 17 (A) of the FIAMLA requires a financial institution to establish policies, controls, and procedures to mitigate and effectively manage the risks of money laundering and terrorism financing identified in any risk assess-ment undertaken by the financial institution. In this respect the financial institution should:

(a) understand its ML and TF risks; and

(b) have in place effective policies, procedures, and controls to:

i) identify,
ii) assess,
iii) understand
iv) mitigate,
v) manage, and
vi) review and monitor those risks in a way that is consistent with the requirements of section 17 of the FIAMLA and the requirements of the FSC Handbook.

A risk-based approach starts with the identification and assessment of the risk that has to be managed. A risk based approach re-quires the financial institution to assess the risks of how it might be involved in ML and TF, taking into account its customers (and the beneficial owners of customers), countries and geographic areas, the

products, services and transactions it offers or undertakes, and the delivery channels by which it provides those products, services and/or transactions.

Through business risk assessments and determination of a risk appetite, XML can establish the basis for a risk0approach does not exempt XML from the requirement to apply enhanced measures where it has identified higher risk factors, as detailed in the FSC Handbook.

Business Risk Assessment

XML must, under Section 17(1) of the FIAMLA identify, assess, understand, and monitor that person's 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 defense. 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 As-sessment lies with the board of directors of the Company.

As explained in the FSC Handbook, a risk assessment involves making a judgement of a number of elements including threat, vul-nerability and consequence. It should also consider the extent of its exposure to risk by reference to a number of additional factors.

A key component of a risk-based approach involves XML identifying areas where its products and services could be exposed to the risks of ML and TF and taking appropriate steps to ensure that any identified risks are managed and mitigated through the estab-lishment of appropriate and effective policies, procedures, and controls.

The business risk assessments are designed to assist XML in making such an assessment and provide a method by which XML can identify the extent to which its business and its products and services are exposed to ML and TF. Good quality business risk assess-ments are therefore vital for ensuring that XML's policies, procedures and controls are proportionate and targeted appropriately.

XML records and documents its risk assessment in order to be able to demonstrate its basis. The assessment is undertaken as soon as reasonably practicable after XML commences business and regularly reviewed and amended to keep it up to date. This risk assessment is reviewed at least annually in case of trigger events and this review should be documented to evidence that an appropriate review has taken place.

Risk management requires a systematic approach, it is a cyclical process. This means that the Company is expected to perform the whole cycle of identification, analysis and testing of the effectiveness of controls at regular intervals. This is because the risks are not static. Risks to the Company may change as a result of both internal and external factors. The Company's activities may for instance be expanded or changed, specific trends may emerge in the financial and economic world, or laws and regulations may be amended.

Since the risks of ML/FT vary from business to business and are not static, it is the responsibility of the Company to identify the vul-nerabilities and risks faced, maintain an up to date understanding of these risks, and develop and implement appropriate strate-gies to mitigate and control those identified risks. This includes adjustment of such mitigation when needed. The appropriate strat-egy in order to manage and control those risks is to have an effective internal compliance culture under the board of directors' ul-timate responsibility.

Any risks that have been identified are properly mitigated by policies, procedures, and controls. XML also documents the mitigating factors and controls put in place to provide an audit trail of how the assessed risks have been mitigated.

Section 17(2) of the FIAMLA requires businesses to assess 6 key areas when undertaking the business risk assessment amongst other risk factors:

l. The nature, scale, and complexity of the financial institution's activities.

2. The products and services provided by the financial institutions.

3. The persons to whom and the manner in which the products and services are provided.

4. The nature, scale, complexity and location of the customer's activities.

5. Reliance on third parties for elements of the customer due diligence process; and

6. Technological developments

As per Section 17(2) (b) of the FIAMLA, financial institutions shall take into account the findings of the National Risk Assessment ('NRA') and any guidance issued in their business risk assessment.

For completeness, the assessment should consider the operational risks, reputational risks and legal risks posed by the use of new technologies in the context of ML/TF. Appropriate action should be taken to mitigate the risks that have been identified.

The anti-money laundering and combatting the financing of terrorism (AML/CFT) Business Risk Assessment Framework can be found in the AML/ CFT Framework adopted by the Company.

Customer Risk Assessments

A customer risk assessment estimating the risk of ML/TF is undertaken prior to the establishment of a business relationship or car-rying out an occasional transaction, with or for, that customer. This risk assessment is documented in order to be able to demon-strate its basis. The customer risk assessment may have to take into account that not all CDD and relationship information might have been collected yet. It is a living document that is revisited and reviewed, as and when more information about the customer and relationship is obtained. The customer risk assessment is done on categories of clients (risk buckets), and it is not necessary to individually risk rate each client should XML deem it appropriate.

The initial risk assessment of a particular customer will help determine:

- The extent of identification information to be sought.
- Any additional information that needs to be requested.
- How that information will be verified; and
- The extent to which the relationship will be monitored on an ongoing basis.

Due care is exercised under a risk-based approach. Being identified as carrying a higher risk of ML/TF does not automatically mean that a customer is a money launderer or is financing terrorism. Similarly, identifying a customer as carrying a lower risk of **ML/TF** does not mean that the customer presents no risk at all. Upon completion of the risk assessment any additional information, evidence or clarification is sought in the event that circumstances remain unclear.

The Customer Risk Assessment and Scoring Methodology can be found in the AML/ CFT Framework adopted by the Company.

Independent Audit

Introduction

Regulation 22(1) (d) of the FIAMLR 2018 requires that financial institutions shall have in place an audit function to review and verify compliance with and effectiveness of the measures taken in accordance with the FIAMLA and FIAMLR 2018.

The Company is a financial institution under the FIAMLA.

According to the FSC Handbook, an AML/CFT independent audit is a vital element of any effective compliance programme for fi-nancial institutions. By virtue of the FIAMLA and FIAMLR 2018, there is a statutory obligation on every financial institution to have in place an audit function which will allow the reporting entity to evaluate its AML/CFT programme and to ascertain whether the es-tablished policies, procedures, systems and controls are adapted with the money laundering and terrorism financing risks identi-fied. The objective of an independent audit is to form a view of the overall integrity and effectiveness of the AML programme, in-cluding policies, procedures and processes.

Conducting a successful independent audit enables a financial institution to ensure that its policies, procedures, and controls remain up to date, recognize deficiencies in regulatory compliance system and develop ways to remediate the breaches in order to be compliant with the prevailing legislation.

Scope of independent audit

In line with international best practices, the independent audit exercise should be risk-based. Independent audit is the Company's final line of defense; therefore, it is vital to ensure that the AML/CFT independent audit is tailored to the Company's risks.

The scope of the independent audit exercise is mainly *a* verification of the AML/CFT risk faced by the financial institution.

Typically, every independent audit should mandatorily test compliance in the following non-exhaustive areas:

- 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 ("TFS"); and
- Suspicious Transaction Monitoring and Reporting.

If the Company relies on automated systems or manual processes to implement its AML/CFT programme, the reliability of these systems and processes should also be considered during the independent audit on a risk basis.

Choosing the Audit Professional

Regulation 22 (1) (d) of the FIAMLR 2018 requires the audit process to be carried out independently. This implies that the person or firm conducting the audit should be independent and must not be involved in the development of a financial institution's AML/CFT risk assessment, or the establishment, implementation or maintenance of its AML/CFT programme.

The audit function should therefore be independent of, and separate from, the operational and executive team dealing with the AML/CFT processes of the Company. An independent audit review may be conducted by an internal or external audit professional.

The person or firm conducting the audit should have the necessary skills, qualifications, relevant experience of the audit process, have a proper understanding of the FIAMLA and its supporting regulations as well as sufficient knowledge of the financial institu-tion's industry. In order to ensure that the audit is properly conducted as required under the FIAMLA and FIAMLR 2018, the audit pro-fessional needs to provide quality recommendations, so that the financial institution can use the findings and recommendations to improve upon deficient areas.

Assessing the "independence" of the audit professional

In all cases, the Company must be satisfied and able to demonstrate that the person or the firm undertaking the audit is ade-quately independent from the area of the business function responsible for risk assessment and AML/CFT programme and ensure that there are no conflicts of interest. Therefore, the independent audit may be conducted by an in-house audit professional not involved in the development and implementation of the AML/CFT programme or outsourced to external accountants or indepen-dent consultants duly regulated or registered by relevant competent authorities

When sourcing an external audit professional to conduct the audit, the Company should conduct some level of due diligence as listed in section 13.3 of the FSC Handbook to confirm the proposed or selected professional candidate has the requisite compe-tence. The criteria considered by the Company when assessing the independence and relevant experience of the external audit professional to effectively perform the auditshould be properly documented and shall be made available to the FSC upon request.

In order to assess the independence of the audit professional, the Company should ensure that the following non-exhaustive perti-nent areas are addressed:

- Was the audit professional involved in the development of the entity's risk assessment? Or the creation, implementation, or maintenance of the AML/CFT programme?

- Does the audit professional have a financial interest in the business? If yes, would their interests be harmed by the results of the audit, or could there be influence over the audit outcome?

- Does the audit professional have any relationship with any shareholder, director, senior management and or employees?

Frequency of the Independent Audit

The frequency and extent of the review should be commensurate with the Company's size, nature, context, complexity and internal risk assessment.

All financial institutions should consider the appropriateness and effectiveness of its compliance arrangements and its policy for the review of compliance at a minimum annually, or whenever material changes to the financial institution or legislative and regu-latory obligations occur. However, the Company can determine for itself the frequency to have its audits conducted. The greater the AML risk of the Company, and of the rate of change of the Company's business, the greater should be the frequency of audit.

For any business that does not have clients during the reporting period, the Company must ascertain the frequency to conduct its independent audit. It may be appropriate that the audit cycle be extended if the Company has no clients and no clients have been on-boarded or exited since the previous independent audit is conducted.

For a Company that is in the process of being wound up, it is recommended that at least one final independent audit is carried out until the Company is no more considered as a reporting entity under the FIAMLA.

The basis for the audit frequency must be clearly articulated in the Company's audit policy and scope.

Key components of the AML/CFT programme

The independent audit report must express views on whether the AML/CFT risk assessment and the AML/CFT programme comply with the requirements of FIAMLA and supporting legislations and whether the programme is functioning effectively in practice as required and intended and has been over the course of the period. The independent audit will involve obtaining a good under-standing of the Company's business, reviewing relevant core documents, file testing, testing of the live application of policies and procedures, and interviewing a cross section of players. The audit process must have sufficient depth and breadth to support the findings and to make the report worthwhile.

Within the framework of the AML/CFT programme itself, the independent audit shall inter alia:

- address the adequacy of AML/CFT risk assessment, including whether it addresses the specific business activities of that particular Company.
- test compliance of the Company's AML/CFT programme, policies and procedures with the FIAMLA, FIAMLR 2018, and the FSC Handbook and a general review of the effectiveness of the compliance function considering the risks identified through the risk assessment.
- assess the employees' adherence to the AML policies and procedures.
- assess employees' knowledge of the AML/CFT laws, regulations, guidance, and policies&. procedures.
- examine the adequacy of Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) policies, procedures and processes, and whether they comply with higher-level internal requirements in the Company. This may include considering the adequacy of on boarding paperwork and considering the adequacy of enhanced measures against the findings of the risk assessment.
- conduct appropriate customer file testing, with particular emphasis on high-risk operations (products, service, customer and geographical locations);
- examine the adequacy of the policies and procedures as well as the processes for identifying and reporting suspicious transactions promptly.
- if an automated system is not used to identify or aggregate large transactions, the audit should include sample test of how the compliance officer conducts monitoring.

- conduct appropriate transaction file testing, including a review of 'not filed' (closed as not suspicious) internal suspicious transactions reports, to determine the adequacy, completeness and effectiveness of the STR filing process.
- examine the adequacy of the policies and procedures as well as the processes for screening for targeted financial sanctions as well as implementing prohibitions, freezing assets, and reporting to competent authorities.
- review how the financial institution is screening for targeted financial sanctions without delay when on boarding clients or conducting transactions and when the lists are updated (within hours), and the appropriateness of periodic screening frequency.
- conduct appropriate testing of TFS screening records, including a review of false positives, to determine the adequacy, completeness and effectiveness of the TFS process.
- examine the integrity and the accuracy of the management information systems use in the AML compliance programme; and
- assess training adequacy including its comprehensiveness, accuracy of materials, training schedule and attendance tracking.

Overall, the audit professional should decide whether the audit coverage and frequency are appropriate to the risk profile of the Company.

Audit outcome, report and recommendations

The audit will result in a signed and dated written report by the audit professional to ensure that the audit programme:

- covers all relevant components of the compliance programme as required under FIAMLA and relevant regulations.
- was adequate and effective throughout a specified period.
- identifies areas where the Company did not meet minimum legal or regulatory standards and include actions that are required to rectify non-compliance as well as identifying areas for recommended changes in behaviour and practice to improve the effec-tiveness of the AML/CFT programme's implementation. This includes an indication of where there are potential failings and a rec-ommended course of action.

A key element of the whole audit process is effective follow-up. Failure to address recommendations and findings of previous audits should be red flagged to the Board or audit committee (if applicable) and will be in any regulatory inspection. The findings of the independent audit report, highlighting recommendations and deficiencies, should be reported to senior management and to the Board of directors.

It is the responsibility of the Board of directors of the Company to take appropriate corrective actions to remediate any issues identified in the independent audit report within the specified timelines.

Filing to the FSC

Financial institutions are not required to file their independent audit report with the FSC periodically. However, the Company shall file its independent audit report for a specified period, upon the request of the FSC.

All independent audit documentation, including, inter alia, work plan, audit scope, transaction testing, should also be properly doc-umented and shall be made available to the FSC upon request.

The FSC may inter-alia, request the following information:

i) whether the Company has adequate policies and procedures in place for independent audit exercise.

ii) what AML/CFT issues have been identified.

iii) What are the controls and procedures in place to ensure that all risks identified are remediated in a timely manner.

iv) when the Company has conducted its last independent audit.

v) when the next independent audit exercise would be scheduled.

vi) whether, from a corporate governance perspective, the Company is considering rotating the audit professional after performing audit after a specific number of years, as it deems appropriate.

Ongoing monitoring for PEP

Once a business relationship has been established with a PEP, on-going monitoring must be conducted on all related transactions to ensure that they are in line with the customer's source of funds and wealth and original account mandate. This can be achieved by requesting for additional information to understand the purpose of a transaction and verifying the provenance of the source of funds and where required, to request for evidentiary documents such as agreements, invoices, bank statements, etc.

Furthermore, quarterly World Check and Internet Check must be conducted on the PEP and evidence of such screening kept on re-cords. Annual reviews must be conducted on all customers identified as PEPs and approved by Board / Senior Management.

The following information and documentation must be reviewed/reconfirmed/updated when conducting an annual review of a PEP client:

- All KYC information.
- The relevance of the EDD conducted initially including reconfirmation of the customer's source of funds and source of wealth.
- Where adverse information such as ongoing litigation or regulatory proceedings were noted as part of the on-boarding information, further checks must be undertaken to ascertain any outcomes or obtain updated information.

Information obtained from the customer may be compared against additional independent sources in order to verify the accuracy of the information. The formal decision and reasons to either maintain or terminate the PEP relationship must be documented.

Factors to consider in establishing/maintaining/terminating a customer relationship with a PEP.

The following are factors, which should be considered in deciding whether to establish/ maintain/terminate a customer relation-ship with a PEP

- funding of the account: are the funds in the Company's account in line with the customer's source of funds and wealth and original account mandate?

- is there a history of suspicious or unexplained transactions?
- is the customer responsive to requests for up-to-date information?

There should be a detailed consideration of the rationale for establishing, maintaining, or terminating the business relationship with the PEP.

[Note - where a customer has been accepted and the said customer or its beneficial owner or its associate or its family member is subsequently found to be, or subsequently becomes a PEP, appropriate EDD and Company Board's approval should be obtained as per above in order to continue such business relationships.]

Connected persons that are PEPs.

Connected persons will include underlying principals such as beneficial owners and controllers.

The Company must apply appropriate EDD measures on a risk-sensitive basis where an applicant for business or customer (or any connected person, such as a beneficial owner or controller) is a PEP, and must ensure that they operate adequate policies, procedures, and controls to comply with this requirement.

The Company must:

- Develop and document a clear policy on the acceptance of business relationships or one-off transactions with such persons and ensure that this is adequately communicated.

- Obtain and document the approval of senior management prior to establishing relationships with such persons.

- Where such persons are discovered to be so only after a relationship has commenced, thoroughly review the relationship, and obtain senior management approval for its continuance; and

- Apply EDD measures to establish the source of funds and source of wealth of such persons

Verification of source of funds and source of wealth

The source of funds and source of wealth are required to be verified to demonstrate a thorough understanding of the source of the initial and ongoing funds and wealth that will pass through the customer's account/product held at the Company. Where initial funding is provided by third parties, the Company should ensure that the relationship between the parties is fully documented and a rationale for such a relationship is recorded and analyzed. If there is no proven rationale for the existence of such a relationship, further due diligence is required.

The source of funds and source of wealth of the PEP must be verified in accordance with the source of funds and source of wealth requirements applicable to that PEP.

Customer Risk Profiling

The Company must identify and assess its potential exposure to inherent ML, TF and sanctions risks introduced as a result of entering into a business relationship with a customer. The Company assesses business relationship risks through a Customer Risk Profiling Toolkit.

The Company will take a number of factors into consideration including but not limited to the following:

- Nature and type of Customer.
- Customer's Nationality (Individual) or Registration Country (corporate)
- Geographical location of the customer's residence / base of activity.

- Customer's source of funds.
- Customer's Activity.
- Transaction Frequency.
- Product type
- High Risk Indicators such as: a) Incomplete CDD, b) Dealing with PEP, c) Dealing with Sanctioned countries, d) Unsupported bank transactions, e) World Check Hit or any adverse info from media or internet, f) EiC or Third-Party Reliance Exceptions (not meeting FSC's minimum requirements)

Risk profiling is applicable to:

- New Customers (at on-boarding stage); and
- Existing Customers.

The following Risk Profiling Classification & Review Date:

- High risk: every 12 months.
- Medium risk: every 24 months; and
- Low risk: every 36 months.

The Company is required to 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.

Third Party Reliance

XML may rely on its Administrator to complete certain CDD measures. The Administrator is regulated, supervised, monitored and is subject to CDD and record keeping requirements pursuant to regulations of the FIAMLA. XML is aware that the ultimate responsibili-ty for CDD measures remains with the Company.

Pursuant to Chapter 8 of the FSC Handbook, a financial institution may rely on relevant third parties to complete certain CDD measures, provided that there is a contractual arrangement in place with the third party. Where reliance is placed on a third party for elements of CDD, the financial institution must ensure that the identification information sought from the third party is adequate and accurate. The CDD information has to be submitted immediately in line with section 17D of the FIAMLA upon on-boarding although the documents can be provided upon request at a later date. Where such reliance is permitted, the ultimate re-sponsibility for CDD measures will remain with the financial institutions relying on the third party

In a third-party reliance scenario, the third party should be regulated, supervised, and monitored and subject to CDD in line with section 17C of the FIAMLA and record keeping requirements pursuant to section 17F of the FIAMLA and Regulation 21 of the FIAMLR 2018 which provides for third party reliance. When reliance is placed on a third party that is part of the same financial group, the financial institution must ensure that the group applies the measures as applicable to regulation 21(4) of the FIAMLR 2018.

Moreover, the financial institution needs to be aware on the level of the country risk when determining in which country (ies) the third party can be based, countries with strategic deficiencies in the fight against money laundering and the financing of terrorism, e.g., those identified by the FATF as having strategic deficiencies. A high-risk country can also be those countries that are vulnera-ble to corruption, and which are politically unstable, the above examples are not exhaustive.

Reliance may only be placed on third parties to carry out CDD measures in relation to the identification and verification of a customer's identity and the establishment of the purpose and intended nature of the business

relationship. Third parties may not be relied upon to carry out the ongoing monitoring of dealings with a customer, including identifying the source of wealth or source of funds. The FSC recommends that regular assurance testing is carried out in respect of the third-party arrangements, to ensure that the CDD documents can be retrieved without undue delay and that the documenta-tion received is sufficient pursuant to section 17(2) (v) of the FIAMLA.

Financial institutions should take steps to ensure that any existing third-party reliance arrangements comply with the applicable AML/CFT legislation in this regard. It is suggested that, where third party reliance arrangements are in place, reporting entities (e.g., funds) receive a report from the administrator about the arrangements that meets those requirements and that the report details the outcome of the testing carried out.

XML shall, pursuant to section 17H of the FIAMLA, with respect to business relationships or transactions involving a high-risk country, apply such enhanced CDD measures as may be prescribed.

In addition, XML shall, where applicable and proportionate to the risks, apply one or more of the following additional mitigating measures to persons and legal entities carrying out transactions involving a high-risk country:

(a) The application of additional elements of enhanced due diligence.

(b) The introduction of enhanced relevant reporting mechanisms or systematic reporting of financial transactions.

(c) The limitation of business relationships or transactions with natural persons or legal entities from the countries identified ashigh-risk countries.

Monitoring Accounts for Suspicious Activity

The Company will manually monitor a sufficient amount of account activity to permit identification of patterns of unusual size, volume, pattern or type of transactions, geographic factors such as whether jurisdictions designated as "non-cooperative" are involved, or any of the "red flags" identified below. The Company will look at transactions, including trading and wire transfers, in the context of other account activity to determine if a transaction lacks financial sense or is suspicious because it is an unusual transaction or strategy for that customer. The Compliance Officer or his or her designee will be responsible for this monitoring, will document when and how it is carried out, and will report suspicious activities to the appropriate authorities. Among the informa-tion the Company will use to determine whether to file a report are exception reports that include transaction size, location, type, number, and nature of the activity. The Company will create employee guidelines with examples of suspicious money laundering activity and lists of high-risk clients whose accounts may warrant further scrutiny. Our CO will conduct an appropriate investiga-tion before a STR is filed.

Emergency Notification to the Government by Telephone

When conducting due diligence or opening an account, we will immediately call law enforcement when necessary, and especially in these emergencies: we discover that a legal or beneficial account holder or person with whom the account holder is engaged in a transaction is listed on or located in a country or region listed on the OFAC list, an account is held by an entity that is owned or controlled by a person or entity listed on the OFAClist, a customer tries to use bribery, coercion, or similar means to open an account or carry out a suspicious activity, we have reason to believe the customer is trying to move illicit cash out of the government's reach, or we have reason to believe the customer is about to use the funds to further an act of terrorism.

Red Flags

Red flags that signal possible money laundering or terrorist financing include, but are not limited to:

- The customer exhibits unusual concern about the Company's compliance with government reporting requirements and the Company's AML policies (particularly concerning his or her identity, type of business and assets), or is reluctant or refuses to reveal any information concerning business activities or furnishes unusual or suspicious identification or business documents.
- The customer wishes to engage in transactions that lack business sense or apparent investment strategy or are inconsistent with the customer's stated business or investment strategy.
- The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.
- Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.
- The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.
- The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs.
- The customer appears to be acting as an agent for an undisclosed principle, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.
- The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.
- The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash, or asks for exemptions from the Company's policies relating to the deposit of cash.
- For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.
- The customer is from, or has accounts in, a country identified as a non-cooperative country or territory by the FATF.
- The customer's account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity.
- The customer's account shows numerous currency or cashier’s check transactions aggregating to significant sums.
- The customer's account has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose.
- The customer's account has wire transfers that have no apparent business purpose to or from a country identified as a money laundering risk or a bank secrecy haven.
- The customer's account indicates large or frequent wire transfers, immediately withdrawn by check or debit card without any apparent business purpose.
- The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another Company, without any apparent business purpose.
- The customer makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer of the proceeds out of the account.
- The customer engages in excessive journal entries between unrelated accounts without an apparent business purpose.
- The customer requests that a transaction be processed to avoid the Company's normal documentation requirements.

- The customer, for no apparent reason or in conjunction with other red flags, engages in transactions involving certain types of securities, such as penny stocks, Regulation S stocks, and bearer bonds, which although legitimate, have been used in connection with fraudulent schemes and money laundering activity (such transactions may warrant further due diligence to ensure the legiti-macy of the customer's activity.).

- The customer's account shows an unexplained high level of account activity with very low levels of securities transactions.

- The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, for no apparent purpose; or

- The customer's account has inflows of funds or other assets well beyond the known income or resources of the customer.

Responding to Red Flags and Suspicious Activity

When a member of the Company detects any red flag he or she will investigate further under the direction of the CO. This may include gathering additional information internally or from third-party sources, contacting the government or filing a Form SAR-SF and STR.

Where a suspicion exists on any transaction, the CO must immediately report the matter to the MLRO. It is vital not to inform any person involved in the transaction or any unauthorised third party that this transaction has been reported to the MLRO as this may amount to an offence under the FIAMLA.

Suspicious Transactions and Reporting

Recognition of Suspicious Transactions

Section 2 of the FIAMLA defines a suspicious transaction as ".... a transaction which -

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

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

(ii) funds linked or related to, or to be used for, 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 word "transaction" is also defined in section 2 of FIAMLA, as follows -

(a) opening an account, issuing a passbook, renting a safe deposit box, entering into a fiduciary relationship or establishing any other business relationship, whether electronically or otherwise; and

(b) a proposed transaction or attempted transaction."

This definition is not exhaustive.

The assessment of suspicion should be based on a reasonable evaluation of different factors, including the knowledge of the Client's business, financial history, unusual pattern of activity, risk profile, background, and behavior. All circumstances surrounding a transaction should be reviewed. It follows that an important precondition for recognition of a suspicious transaction or activity is that the employees of the Company must know enough about the business relationship to recognize that a transaction or activity is unusual.

In case of suspicion, an employee is not expected to know the exact nature of the underlying criminal offence (called the predi-cate offence), or that the particular funds were those arising out of the crime or being used to finance international terrorism. The simple rule is, where a transaction raises any suspicion, the employee should as a first step request more information from the customer about the circumstances surrounding the transaction. He must decide if the explanation received is reasonable and legitimate and if not, report the transaction to the MLRO.

Internal Reporting of Suspicious Transactions

It is a statutory obligation on all employees to report suspicious transactions promptly and directly to the MLRO or to his deputy in his absence. This should normally be done via an Internal STR Form ("ISF"),

In urgent circumstances, an internal STR may be report-ed to the MLRO verbally and followed by the ISF. Failure to report suspicious transactions will constitute a breach of the FIAMLA and may entail criminal sanctions and interference with the preparation or submission of an internal STR may lead to disciplinary sanctions.

The MLRO shall be of sufficiently senior status and shall have relevant and necessary competence, authority, and indepen-dence. The contact details of the MLRO and those of the Deputy MLRO are provided below:

	MLRO	Deputy MLRO
Name		
Email		
Telephone		

All suspicions reported to the MLRO will be recorded in writing, even if the suspicion is reported verbally. The internal STR should include full details of the Client and a full statement as to the information giving rise to the suspicion. The MLRO will acknowledge receipt of the internal STR and, at the same time, provide a reminder of the obligation to do nothing that might prejudice enquiries that is, '**tipping off**'the customer which is a criminal offence under the FIAMLA.

The MLRO will validate all internal STRs before submissions to the FIU and make sure that reports are not made in bad faith, maliciously and without reasonable grounds.

Reporting of Suspicious Transactions to the FIU

Once the MLRO receives an ISF from the relevant staff member, he will determine whether the information contained in the internal STR gives rise to a suspicion that a client is engaged in ML and/ or TF. In this respect, the MLRO shall have unfettered access to any or all information which he may need in considering his report. In making his judgment, the MLRO will consider all relevant informa-tion that has been made available to him.

If, after completing the review he believes that there is no fact(s) which can negate the suspicion, he has the obligation to report the transaction in writing to the FIU through the latter's online platform, GoAML. If, on the other hand, the MLRO does not find it appropriate to report a transaction to the FIU, he will document the reasons for not doing so. This information may be required to supplement the initial report or as evidence of good practice and best endeavors if, at some future dates, there is an investigation, and the suspicions are confirmed. On-going communication between the MLRO and the reporting staff is important.

The MLRO is expected to act autonomously, promptly, honestly, and reasonably, and to make any determination in good faith.

Reporting Obligations and Offences

Section 14(1) of the FIAMLA provides 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."

Pursuant to section *14(3) of* the *FIAMLA*

"Where a reporting person *or* an *auditor* -

(a) becomes aware of a *suspicious* transaction; *or*

(b) ought *reasonably* to *have become aware of* a *suspicious* transaction,

and he fails to make a report to FIU of such transaction not later than 5 *working days* after the *suspicion* arose, *he shaff* commit an offence *and shaff,* on conviction,

be liable to *a fine* not *exceeding* one *miff*ion rupees.

and to imprisonment *for a* term not *exceeding* 5 *years."*

AML Record Keeping

Responsibility for AML Records and SAR Fifing

Our Compliance Officer and his or her designee will be responsible to ensure that AML records are maintained properly, and that SARs are filed as required. We will maintain AML records and their accompanying documentation for a least seven years. We will keep other documents according to existing BSA and other record-keeping requirements.

Training Programs

The Company will develop ongoing employee training under the leadership of the Compliance Officer and senior management in accordance with applicable laws. Our training will occur on at least an annual basis. It will be based on our Company's size, its customer base, and its resources.

Our training will include, at a minimum: how to identify red flags and signs of money laundering that arise during the course of the employees' duties; what to do once the risk is identified; what employees' roles are in the Company's compliance efforts and how to perform them and the Company's record retention policy;

we will develop training in our Company, or contract for it. Delivery of the training may include educational pamphlets, videos, intranet systems, in-person lectures, and explanatory memos. We will maintain records to show the persons trained, the dates of training, and the subject matter of their training.

We will review our operations to see if certain employees, such as those in compliance, margin, and corporate security, require specialized additional training. Our written procedures will be updated to reflect any such changes. Regular training will be provided to all employees on AML/CFT. All employees should attend the training sessions which will be delivered by the MLRO and/or Compliance Officer. The main objective of the training is to generate and maintain a satisfactory awareness level and vigilance that would help identify any suspicious transaction.

Business Continuity Plan

Background

While it is recognized it is not possible to create a plan to handle every possible event, it is the intent of this Company to set up a framework to be used in most likely scenarios. It is also the intent that this framework provides guidance as to how to respond should an unforeseen situation occur.

Business Description

The Company was incorporated in Mauritius on [14 March 2023] and holds a Global Business License Company under the Financial Services Act 2007 ("FSA") and is authorized to operate as an Investment Dealer under the Securities Act 2005.

Company Policy

Our Company's policy is to respond to a Significant Business Disruption (SBD) by safeguarding employees' lives and Company property, making a financial and operational assessment, quickly recovering and resuming operations, protecting all of the Company's books and records, and allowing our clients to transact business. In the event that we determine we are unable to continue our business, we will assure clients prompt access to their funds and securities.

Significant Business Disruptions (SBDs)

Our plan anticipates two kinds of SBDs, internal and external. Internal SBDs affect only our Company's ability to communicate and do business, such as a fire in our building or the death of a key member of the Company. External SBDs prevent the operation of the securities markets or a number of firms, such as a terrorist attack, a city flood, or a wide-scale, regional disruption including epidemics, pandemics and outbreaks. Our response to an external SBD relies more heavily on other organizations and systems, such as the custodian we use.

In the event of an internal SBD such as a fire or flood in one of our offices, employees are instructed to work remotely until the building is safe for use again. An internal SBD such as a death of a key member of the Company will not warrant employees to work remotely and the manager in charge will follow the guidelines in our Key Man Policy and work in conjunction with our administrator.

In the event of an external SBD, if local or central governments deem it necessary to stay home from work and avoid public places, all employees are instructed to work remotely. Employees should be available by e-mail and telephone if possible.

Approval and Execution Authority

[Insert Name], as CO, is responsible for approving the plan and for conducting t he required annual review. The CO has the authority to execute this BCP

Plan Location and Access

Our Company will maintain copies of its BCP and annual reviews, and all changes that have been made to it. A physical copy of the BCP will be stored with the Company's Written Policies and Procedures Manual, which is kept on TUL's Dropbox in the TUL Compliance folder.

Alternative Physical Location(s) of Employees

n the event of an SBD that makes it impossible or impractical to use the Company offices, all employees are instructed to work remotely at their homes or in another safe location. Employees should avoid using public Wi0Fi and utilize their VPNs.

Data Back-Up and Recovery (Hard Copy and Electronic)

Our Company maintains its primary hard copy books and records and its electronic records at:

c/o IQ EQ Fund Services (Mauritius) Ltd
33 Edith Covell Street
Port-Louis, 11324, Mauritius
Phone: (230) 212 9800

IQ EQ Fund Services (Mauritius) Ltd is responsible for the maintenance of these books and records.

The Company keeps all of its data stored electronically on a cloud-based system which is backed up instantaneously.

Operational Assessments

Operational Risk

In the event of an SBD, we will immediately identify what means will permit us to communicate with our clients, employees, critical business constituents, and regulators. Although the effects of an SBD will determine the means of alternative communication, the communications options we will employ will include our website, telephone voice mail, secure e-mail, etc.

Regulatory Reporting

Our Company is subject to regulation by the FSC. We file reports with our regulators using paper copies in the mail, and electroni-cally using fax, e-mail, and the Internet. In the event of an S BD, we will check with the relevant regulators to determine which means of filing are still available to us and use the means closest in speed and form (written or oral) to our previous filing method.

In the event that we cannot contact our regulators, we will continue to file required reports using the communication means available to us.

Regulatory Contact

The Chief Executive
Financial Services Commission
54 Ebene Cybercity
Ebene
Mauritius
230-403-7000

Updates and Annual Review

Our Company will update this plan whenever we have a material change to our operations, structure, business or location or to those of our brokerage firm. In addition, our Company will review this BCP annually, to modify it for any changes in our operations, structure, business, or location or those of our brokerage firm.

Client Due Diligence Checklist

Please refer to the AML-CFT Framework of XML.

Employee Attestation

I attest that I, a supervised person of XML, have read, understood, and agree to comply with the rules in the Policies and Procedures Manual and Code of Ethics.

Supervised Person Name		Date
Supervised Person Signature		
Supervisor Signature		