vt markets

Anti Money Laundering & Compliance Manual

VT Markets Limited

Company no. 201902 GB

Level 2, Suite 201, The Catalyst, 40 Silicon Avenue,
Ebène, Republic of Mauritius

www.vtmarkets.com
info@vtmarkets.com

Table of Contents

1. Purpose

VT Markets Limited (the "Company") has implemented this Anti-Money Laundering and Compliance Manual (hereinafter referred to as a "Manual") to;

1. Prevent money laundering and terrorist financing in relation to its business; and
2. Structure the policies and procedures that the compliance department shall follow.

The purpose of this Manual is to establish the general framework with Mauritius for the fight against money laundering and financing of terrorism. The Policy serves as a high-level resource of reference to the Company's employees.

The Company is licensed by Financial Services Commission, Mauritius pursuant to section 29 of the Securities Act 2005 and Rule 4 of the Securities (Licensing) Rule 2007. This document has been classified as confidential and should be used strictly for internal business purposes.

1.1 Manual Summary;

The main objectives of the Manual are:

a. To comply with the AML regulations and other applicable regulations of Mauritius;

b. To abide by the rules issued from time-to-time by the Mauritius FIU, FSC and to assist the regulatory authorities in combating Money Laundering and Terrorist financing;

c. To abide by the FATF recommendations and Mutual Evaluations Report by ESAAMLG, especially those related to KYC;

d. To monitor the compliance culture and effective reporting structure;

e. Pursuant to Regulations 22 (1) of the FIAML Regulations 2018 and the Code, the Company has designated a Compliance officer (CO);

f. Pursuant to Regulations 26(1) and 26 (2) of the FIAML Regulations 2018 and the Code, the Company has designated a Money laundering Reporting Officer ("MLRO") and Alternate Money Laundering Reporting Officer ("AMLRO")

g. To ensure the Company and all employees are required to complete AML Training upon commencement, annually thereafter and as/when there are changes to relevant legislations;

h. To comply with all sanctions regimes and implement systems to check and validate any transactions that may be directly or indirectly linked to sanctioned individual or entity;

i. Regular reviews of the Policy to ensure ongoing compliance with regulatory updates;

2. Scope of Anti-Money Laundering and Compliance Manual;

The Company requires all directors, officers and employees to read, understand, and follow this Policy in the course of performing services for the company.

The Manual is a structured set on the following legislations/codes/guidelines;

Legislations;

- The Financial Intelligence and Anti-Money Laundering Act 2002;
- Financial Intelligence and Anti-Money Laundering Regulations 2018;
- The Prevention of Terrorism Act 2002;
- The Financial Services Act 2007;
- The Convention for the Suppression of the Financing of Terrorism Act 2003;
- The United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019;
- The Anti-Money Laundering and Combatting the Financing of Terrorism (Miscellaneous Provisions) Act 2020;
- The Prevention of Corruption Act 2002;
- The Companies Act 2001; and
- The Trusts Act 2001.

Guidelines

- Financial Intelligence and Anti-Money Laundering Regulations 2003;
- AML/CFT Handbook issued by FSC, January 2020;

Code/Standards

- The FSC Code on the Prevention of Money Laundering & Terrorist Financing (March 2012 and updated as 2017);
- The FSC Competency Standards (October 2014); and
- The FSC Code of Business Conduct (01 October 2015).

2.1 Compliance officer and its Responsibilities;

The Company have appointed a Compliance officer (the 'CO') for the implementation and ongoing compliance of the Company with internal programmes, control and procedures. The CO appointed work towards by assessing controlling/mitigating compliance and reputational risk. The CO is empowered with full oversight of any monitoring and testing.

CO will be responsible for the following but not limited to

- Implementing Customer Identification Program;
- Carrying CDD checks on legal entities and natural persons;
- Implementing internal programmes, compliance systems, controls and procedures;
- Managing complaints by client;
- Assisting FSC and other regulatory bodies with investigations;

- Ensuring compliance with regulatory requirements;
- Design training programs on AML/CFT and other compliance related matters and deliver training to staff thereon and promote a strong and modern compliance culture;
- Monitor key internal controls, carry out preliminary assessment and report to the board;
- Provide compliance advise for products and/or services to ensure compliance with laws and rules;

2.2 The MLRO and Its Responsibilities;

The Company has appointed a Money Laundering Reporting Officer (the 'MLRO') to implement and monitor the provisions of the AML code and any other law relating to money laundering or financing of terrorism. The Company has also appointed a Deputy Money Laundering Reporting Officer (the 'DMLO'), the DMLRO will fulfil the duties in the absence of MLRO.

The MLRO appointed have the necessary skills and expertise for the role. The MLRO operates independently and reports to the Directors on administrative matters only. On all compliance related matters, the MLRO will report exclusively to the Board of the Company.

The MLRO is empowered to intervene in any transaction, project or course of conduct where there is reason to believe that a breach of legal or regulatory or internal policy, standard or limit may occur or have occurred.

In accordance with Section 3.4 of the AML Code, the MLRO and DMLRO within the organisation shall be the dedicated person to receive suspicious or unusual transaction reports from employees handling transactions within the Company and who decides, on his own accord, how to treat those said suspicious or unusual transactions reported to it

MLRO will be responsible for the following but not limited to;

- The design and implementation of as well as updating the Manual as required;
- Training of Directors, officers and employees
- Maintaining necessary and appropriate records;
- Receive and examine suspicious transaction reports from employees of the Company;
- Review and report transactions, it considers suspicious to FIU;
- Independent testing of the operations of the AML & Compliance Policy.

3. Governance

3.1 International governance standards;

The Policy must be read in conjunction with international governance standards and best practices recommended by;

a. Eastern and Southern African Money-Laundering Group (ESAAMLG).

b. Financial Action Task Force (FATF).

3.2 Financial Services Commission;

The Financial Services Commission, Mauritius (the 'FSC') is the integrated regulator for the non-bank financial services sector and global business. Established in 2001, the FSC is mandated under the Financial Services Act 2007 and has as enabling legislations the Securities Act 2005, the Insurance Act 2005 and the Private Pension Schemes Act 2012 to license, regulate, monitor and supervise the conduct of business activities in these sectors.

Duties of the Company towards the FSC;

a. Ensure that the Company will operate fairly, transparently and in an orderly way;
b. The Company will handle and manage conflicts between its commercial interests;
c. Monitor the conduct of customers;
d. The Company will take all necessary steps to make sure that each of its officers, are fit and proper person;
e. Assist and ensure that customers abide to the FSC licensing conditions;
f. Notify the FSC in case there is change in the shareholding, in UBO (ultimate beneficiary owner), in company secretary, in company's name and in registered office address.
g. Provide the FSC with information and notification of events concerning the business;
h. Setting out clear guideline and timescales for other expected matters and events, which should be notified to the FSC and other authorities;
i. Remaining available for any queries from the FSC to assist the FSC during onsite visits or information collection; and
j. Keeping up to date with current affairs and issues happening in the industry.

3.3 Registrar of Companies (ROC) and Business Registration Department;

The Corporate and Business Registration Department is a government office, which falls under the aegis of the Ministry of Finance and Economic Development. The Registrar of Companies is a public organisation who may delegate any of his duties under the Companies Act 2001 to any public officer appointed to assist him in the execution of his functions.

The Registrar of Companies and Business Registration Department administers:

a. The Companies Act 2001;
b. The Business Registration Act 2002;
c. The Insolvency Act 2009;
d. The Limited Partnerships Act 2011 and The Foundations Act 2012.

3.4 The Financial Intelligence Unit;

The Financial Intelligence Unit (the "FIU") has been established under section 9 of FIAMLA in August 2002. It is the central Mauritian agency for the request, receipt, analysis and dissemination of financial information regarding suspected proceeds of crime and alleged money laundering offences as well as the financing of any activities or transactions related to terrorism to relevant authorities.

The MLRO and the DMLRO of the Company should be duly appointed and the FIU duly informed. In addition, the MLRO and DMLRO should be duly registered on all systems operated by the FIU for any regulatory reporting.

3.5 Regulatory inspection protocols;

On-site inspections and reviews are routine regulatory practices for regulators. The regulator may or may not send an official letter informing the Company on the date that the inspection will start and the person designated to lead the inspection at the Company.

3.6 Communication with Regulators;

All communication with supervisors and regulators should be undertaken within a disciplined framework. Communication may accordingly be undertaken by nominated employees as determined by the Compliance officer and the Directors. Employees are requested to contact Compliance Department should they require any clarification in this regard.

All correspondences, be it significant or not, are routed to the Directors which is then disseminated to the Compliance officer for proper action and follow up process. This provides an ease to follow up, but also ensures alignment and that Compliance is kept appraised of all dealings with the Financial Services Commission, or any other regulator, in the event of any query received from them.

3.7 Financial Services Act 2007, Securities Act 2005 and relevant circulars, Directives and guidance notes;

The Financial Services Commission issue Circulars, Directives and Guidelines as well as rules in terms of the Financial Services Act 2007 and the Securities Act 2005 from time to time.

Compliance Department ensures that these Circulars, Directives and Guidance notes are distributed to the relevant personnel and that the contents thereof are noted. The onus is on the business unit to ensure that the provisions contained therein are adhered to. The guidelines and rules are also available to staff.

3.8 Annual AML Plans;

The MLRO will submit an annual report to the board on key deliverables based on;

a. Review of the level of compliance with the money laundering procedures within the Company, related particularly to the identification of Customers, ongoing monitoring, record keeping, reporting of suspicious transactions and training.

b. Number of internal staffs report on Suspicious Transaction Report (iSTR) received.

c. Number of Suspicious Transaction Report (STR) made to the FIU.

d. List of staffs who have failed to satisfactorily complete the relevant money laundering training.

3.9 AML & Compliance Manual Implementation Requirements;

Each major change of the Company's AML policy is subject to approval by the board. This policy will be reviewed annually and revised as needed.

4. Risk Based Approach

To Assist in determining the level of due diligence to be exercised with regard to the Client, a client risk categorisation will be done. The Clients are categorised into "High Risk", "Medium Risk", and "Low Risk". The risk categorisation takes into consideration the following risk factors:

4.1 Customer Risk;

When identifying the risk associated with clients, the Company considers the risks related to:

a. Any Politically exposed persons PEP's (domestic and foreign);
b. Customers who are identified as being persons or entities which support terrorist activity or are named in government lists or with credible sources in respect of corruption and/or criminal activity;
c. Customers (not necessarily PEPs) based in, or conducting business in or through, a high-risk geographic location, or a geographic location with known higher levels of corruption or organised crime, or drug production/distribution
d. Customers and the customers' beneficial owner's business or professional activity, and
e. The client's and the client's beneficial owner's nature and behaviour;

4.2 Geographical Risk;

When identifying the risk associated with geographical risk, the Company considers the risks related to:

a. Countries identified by credible sources (such as FATF) as providing funding or support for terrorist activities or who have terrorist groups working within the country;
b. Countries subject to sanctions, embargoes or similar measures issued by, for example the U.N., EU and OFAC
c. Countries identified by the FATF as non-co-operative countries and territories;
d. Countries having significant levels of corruption or other criminal activities such as narcotics, arm dealing, human trafficking, illicit diamond trading, etc
e. Countries identified to support terrorist activities, or have designated terrorist organizations operating within their country

4.3 Delivery Channel Business Risk;

When identifying the risk associated with delivery channel business risk, the Company will considers the risks related to:

a. The channels through which the Company establishes a business relationship or through which transactions are carried out. Channels that favour anonymity increase the risk of Money Laundering /Terrorist Financing if no measures are taken towards this.

b. In the cases where interaction with the client takes place on a non-face to face basis, technological measures have been put in place to mitigate the heightened risk of identity fraud or impersonation present in these situations. These measures allow the Company to establish whether the client providing the relative identification details is actually the person he alleges to be.

4.4 Transaction Risk;

The Company will identify the risk of Money Laundering /Terrorist Financing associated to the services and transactions offered/processed to/for their clients. Identified risk may arise due to unusual activity and request which lack commercial sense.

When identifying the risks associated with services/transactions, the Company considers the risks related to:

a. the level of transparency the service/transaction affords;
b. the complexity of the service/transaction; and
c. the value or size of the service/transaction,

4.5 Risk Scoring;

The risk scoring is ranged from 0 to 80 with 0 being the lowest and 80 being the highest risk posed to the Company.

4.5.1 Risk Scoring Table;

The weight assigned to each risk factor to ascertain the overall total risk rating of each Customer is judgemental and based on the non-exhausting list of risk factors stated in Annexure 3.

61-80	41-60	0-40
High	Medium	Low

The average of risk factor classification as presented in section 4.1, 4.2, 4.3, and 4.4 should be calculated and inputted in the Risk Assessment Table (Annexure 4). The sum of score should fall in one of the risk assessment categories (High/Medium/Low).

For clients who are identified as PEPs or those are associated to High-risk countries should be classed as High-risk.

4.5.2 Total Scoring for Risk Classification;

61-80	41-60	0-40
High	Medium	Low

This rating will determine the level of due diligence and the monitoring process (as per table 4.5.3) the Company will adopt to mitigate the risk.

The overall responsibility for the risk assessment and implementation lies with the MLRO. If at any stage, the MLRO chooses to override the manual or automated risk assessment scores/results, then the rationale along with any information used should be documented and appropriately filed.

4.5.3 Applicable level of due diligence & monitoring;

Total Risk Scoring	61-80	41-60	0-40
Risk Level	High	Medium	Low
Due Diligence Level	EDD	CDD	CDD
Monitoring	Quarterly	Every 1 Year	Every 2 Year

The results of the above process should be documented in the "Client Risk Assessment" from (template of the form can be found in Annexure 4) and placed into the file of each Client.

5. Customer Due Diligence

An application must be made by completing and submitting Account Application form (different for Natural person and Legal Entity) and a fully executed Client agreement.

Prior to offering services to customer, the Company ensures that the customer is of good standing and reputation. The profile of the potential customer is analysed via application form. Application form, completed by the customer, is a legal document. The information contained therein is important and often supports the identification information provided by the customer.

The Customer On-boarding team will ensure that all sections of Application form are completed in full; if the information is missing, the Application form will be returned to the customer for completion.

All Customers are subject to screening methods set out below. The documentary evidence to be requested is set out in the Annexure 1 which specifies the requirements for Customers.

The Company ensures;

a. collect certain identification information from each customer who opens an account;

b. utilize risk-based measures to verify the identity of each customer who opens an account; and

c. record customer identification information and the verification methods and results;

5.1 The customer acceptance relies on the following fundamental principles;

a. Each document must be identified as true copies of the original documents.

b. documents can be certified by one of the following;

1. Where the applicant meets with senior employees of the Company who have sight of relevant original documentation, the senior employees may take copies of the

verification of identity documentation and certify them personally as true copies of the original documentation.

2. Where there is no personal contact, obtain a copy certified as a true copy by an Attorney, a Barrister, a Notary or a Chartered Accountant.

3. The certifier should sign the copy document and clearly indicate his/her name, address and position or capacity on it together with contact details for identifying the certifier.

c. Application will not be accepted if the identification proves to be incomplete. For all accounts, if applicable for any person, entity or organisation opening a new account and whose name is indicated on the account;

1. Name, incorporation number, legal status, date and country of incorporation or registration (for an entity other than an individual);

2. Date and place of birth (for an individual)

3. Occupation, public position held and where appropriate, the name of the employer (for an individual) or Anti-Money Laundering and Counter-Terrorism Financing Policy (for an entity other than an individual)

4. A current address, which will be residential (for an individual) or registered office address and principal place of business (where different from the registered office, for an entity other than an individual)

5. Passport number and country of issuance, identification card number and country of issuance of any other government issued document evidencing nationality or residence and bearing a photograph or other similar safeguard e.g. national identity cards, current valid passports or current valid driving licenses; and

6. The identity of underlying principles (including beneficial owners, controllers, directors or equivalent) with ultimate effective control over the capital or assets of an entity other than an individual in addition to evidence that any person who purports to act on behalf of the legal person is duly authorized and identify that person.

d. Where the underlying principals are not individuals, the Company shall investigate further to establish the identity of the natural persons ultimately owning or controlling the business. When opening an account for a foreign business or enterprise that does not have identification number, the Company will request alternative government approved documentation certifying the existence of the business or enterprise.

e. If potential customer refuses to provide the information described above or such information as the Company may require or appears to have intentionally provided misleading information, the Company shall not open a new account and, after considering the risks involved, will consider closing any open account(s) of an existing customer.

f. Risk profile of the Customer is determined based on those documents. If the risk is found to be higher than average, enhanced due diligence may be necessary before on boarding the customer and/or ongoing close monitoring of Customers transactions might be necessary or sufficient. The Company ensures to all reasonable and practicable that the sanction screening of each Customer as per section 5.5.

g. After the final assessment and before entering in a business relationship with the customer, the customer acceptance sheet must be signed by the Compliance Officer, thus giving acceptance to proceed the on boarding of Customer.

h. All documents will be recorded for a minimum period of seven (7) years from the date of the on boarding of the Customers.

5.2 Simplified Due Diligence

The Company reserves the right to proceed with a Simplified Due Diligence (SDD) where lower risks have been identified and the SDD shall be commensurate with the lower risks factors in accordance with the regulatory guidelines as applicable.

An example of simplified CDD measure could be not requiring CDD documentation for beneficial owner of publicly listed entities.

5.3 Enhanced Due Diligence;

Customers which present a higher risk to the Company will be subjected to enhanced due diligence. The enhanced due diligence process will involve further consideration of all documentation and risk factors associated to the Customer. It may require a Customer On-boarding team to seek clarification or additional documentation from the Customer, which includes obtaining additional supporting documents. This process is designed to assure that the Company has secured a greater level of verification and understanding of the Customer.

The Compliance Officer shall maintain a negative list of entities circulated by the Mauritius Government, FIU and by the equivalent jurisdiction authorities.

5.3.1 **Enhanced CDD shall be done as a result of the following trigger events:**

a. when Customer documentation standards change substantially;

b. there are doubts about the veracity or adequacy of previously obtained information;

c. there is a material change in the way that an account is operated or in the manner in which the business relationship is conducted;

d. there is a suspicion of Money Laundering / Terrorism Financing;

e. where the applicants are from Countries/jurisdictions identified by the Financial Action Task Force (FATF) as being 'non-cooperative' or flagged by the FSC and/or Central BANK, the Company shall carry out enhanced checks, using automated software system, against databases of the United Nations Security Council Sanctions, Politically Exposed Persons (PEP), Unilateral Sanction of HM Treasury of UK, Adverse Media and others. Additional documentation may also be sought regarding the sources of wealth/source of funds, if deemed necessary.

5.3.2 **Enhanced Due Diligence Measures;**

a. obtaining additional Customer information, such as the customer's reputation and background from a wider variety of sources before the establishment of the business relationship and using the information for the risk profiling;

b. carrying out additional searches (e.g., internet searched using independent and open sources) to better assess the customer risk profile;

c. carrying out additional searches focused on financial crime risk indicator (i.e., negative news screening) to better assess the customer risk profile;

d. undertaking further verification procedures on the customer's beneficial owner to better understand the risk that the customer's beneficial owner may be involved in criminal activity;

e. obtaining additional information about the customer's source of wealth or the source of funds involved in the transaction;

f. verifying the source of funds or wealth involved in the transaction or business relationship to seek to ensure they do not constitute the proceeds of crime;

g. evaluating the information provided with regard to the destination of funds and the reasons for the transaction;

h. seeking and verifying additional information from the customer about the purpose and intended nature of the transaction or the business relationship;

i. increasing the frequency and intensity of transaction monitoring.

5.3.3 **Enhanced Due Diligence Process;**

Where it is determined that enhanced due diligence should be applied, the process will be as follows;

a. Compliance will conduct a thorough investigation to determine the source of the client's and each beneficial owner's wealth;

b. Check the validity of the account registration details;

c. Re-verify KYC information;

d. Review any linked accounts;

e. Analyse the customer's past transactions and possibly monitor future transactions if deemed necessary;

f. Identify the purpose or nature of specific transactions;

g. Check IP address where possible to detect any suspicious connection sources;

h. Determine if any suspicious activity report should be lodged in accordance with procedures.

5.4 Politically Exposed Persons (PEPs) Screening;

PEP's receive additional focus in AML Code, and this is also reflected in this Manual and training. PEP's noteworthiness arises from the risk of bribery and corruption.

a. Politically Exposed Person means;

1. an individual who is or has been during the preceding 3 years, entrusted with a prominent public function in;

I. Mauritius;

II. any other country; or

III. an international body or organisation;

2. an immediate family Customer of a person referred to in section 5.4.a.1.

3. a close associate of a person referred to in section 5.4.a.1.

4. PEP also means a "foreign PEP", being a natural person who is or has been entrusted with prominent public functions by a foreign country, including Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials and such other person or category of persons as may be specified by a supervisory authority or regulatory body after consultation with the National Committee;

5. The meaning of PEP further extends to "international organisation PEP", being a a person who is or has been entrusted with a prominent function by an international organisation and includes members of senior management or individuals who have been entrusted with equivalent functions, including directors, deputy directors and members of the board or equivalent functions and such other person or category of persons as may be specified by a supervisory authority or regulatory body after consultation with the National Committee;

b. Politically Exposed Persons includes;

1. head of state, head of government, ministers and other and senior politicians;

2. senior government or judicial officials;

3. ambassadors and diplomats;

4. Customers of the boards of central banks;

5. Customers of state-owned corporations;

6. important political party officials.

c. Immediate family Customers of Politically Exposed Persons includes;

1. a Spouse;

2. a partner, that is an individual considered by his or her national law as equivalent to spouse;

3. children and their spouses or partners;

4. parents and;

5. siblings.

5.5 Performing PEPs Due Diligence Procedures

a. Where a customer is identified as a PEP, the Company collects and verify KYC information and undertakes enhanced due diligence measures. The Company then determined whether the PEP poses an AML/CFT risk. If classified as PEP, the compliance officer informs the Board regarding the confirmed PEP.

b. In case of confirmed PEPs its Company' Board's decision not to proceed with onboarding of such client.

c. In case the customer becomes PEP during ongoing business relationship and his/her PEP status is confirmed during ongoing monitoring or annual review, it is an obligation of the Compliance officer to report to the Board.

d. The Board in its turns take the decision regarding the business relationship with the client.

e. the Board will not continue the business relationship and will terminate the business relations. However, a time of One Months will be given to the client to close any open positions with the company.

f. All records of terminated business will be kept for 7 years.

5.6 Ongoing Monitoring;

This Manual sets appropriate procedures in order to monitor the Customer data, information, and transactions. Compliance Officer will conduct ongoing monitoring throughout the Customer business relationship with the objective of;

a. Ongoing Customer Review: for some dedicated high risk and medium risk customers, a periodically risk-based review is carried out to ensure that customer-related data or information is up to date. The purpose of these reviews is to identify any significant changes to the corporate structure, management and activities of the customer. The frequency of such reviews is determined by the customer's risk category. The review of the customers through Ongoing Customer Review Form (template of the form can be found in Annexure 5) is done with the following frequency;

    1. Low-Risk clients are re-assessed every two years

    2. Medium-risk clients are re-assessed every year; and

    3. High-risk clients are re-assessed quarterly.

    Notwithstanding these timescales, should any employee become aware of a change in the circumstances of a client, for example change of resident country, ownership structure, source of income from high-risk jurisdiction, management or move into a new employment or area of business. If this information could affect the risk assessment of the client, then the CO and MLRO should be informed. The CO and MLRO will then decide if there is the need to re-evaluate the client risk assessment.

b. Scrutinising transaction monitoring;

    Transaction monitoring is conducted to detect transactions which are significant or suspicious will monitor a sufficient amount of account activity to permit the 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 in Annexure 6. 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.

c. Record Keeping

Evidence of all monitoring undertaken by the Company will be retained for a period of at least seven years from the date of the review.

5.7 Sanctions Screening;

a. Sanction screening is to ensure compliance with the applicable sanctions against persons and entities. the Company has put in place to compare the entity name, beneficial owners, directors and authorised persons with official list of;

1. The US Department of the Treasury Office of Foreign Assets Control (OFAC) sanctions list; https://sanctionssearch.ofac.treas.gov/
2. The UK HM Treasury (HMT), office of Financial Sanctions implementation, "consolidated list of targets"; https://ofsistorage.blob.core.windows.net/publishlive/ConList.html
3. The United Nations (UN) Security Council consolidated sanctions list; https://scsanctions.un.org/search/ ; https://scsanctions.un.org/consolidated/
4. Financial Action task force, Member countries;
5. All other applicable sanctions laws and regulations in the Mauritius jurisdiction; and
6. IBAN Check for screening of Shell Banks. No business relationship is established if customer presents shell Banks details for account application. https://www.iban.com/

b. Any potential match returned is investigated by Compliance Officer to understand if it is a match or false. If the potential match does return as a positive match, Enhanced Due Diligence may be required by the Customer to furnish the Company with additional information as and when necessary.

c. Compliance Officer may also take appropriate measures should the business relationship result in a risk, which may include;

1. Immediately terminate the relationship with the Customer and inform the FSC.
2. If Compliance officer decides to maintain the relationship with the Customer, Enhanced Due Diligence will be done, and a full report will be submitted to the Board detailing the reasons to maintain the relationship with the Customer.

5.8 Source of funds and Source of Wealth;

a. Understanding the customer's source of funds and source of wealth is an important aspect of customer due diligence. Such identification allows the prevention of risk and money laundering. It is important to distinguish between the source of funds/property and the source of wealth.

b. Appropriate measures to establish source of funds for each Customer at the Company are placed. The Company ensures the consistency between the information it holds and the nature of transactions or proposed transactions. Where there is any indication of abnormal or potentially suspicious activity within the context of the product or service being provided, the Company takes additional measures to verify the information obtained.

c. In addition to establishing the source of funds, the Company takes adequate measures to establish the source of wealth of clients and beneficial owners.

d. Enhanced due diligence (EDD) will also be carried out in respect of Customer, other than PEPs, which due to their nature entail a high risk of money laundering or terrorist financing.

e. The Company will also request from the prospective customer a signed declaration of source of funds detailing the provenance of such funds and affirming that the funds do not emanate directly or indirectly from any criminal or unlawful means.

f. The Company will also ensure that the source of funds is logical and backed by supporting documentations. Annexure 6 for examples of details required when assessing the source of funds, together with suggested documentary evidence.

6. Reporting of Suspicious Transactions

6.1 Transaction Screening and Monitoring;

the Company will do ongoing transaction monitoring and sanction screening of all Customers and beneficiaries, single transaction monitoring and risk assessment, profiling, and Customer transactional behaviour. The alerts generated upon verification by Compliance Officer, EDD will be applied and appropriate actions in case of suspicion.

6.2 iSTR;

An Internal Suspicious Transactions Report (iSTR) is raised by the officer, employees, or internal audit team (the Company's team members), to the MLRO in case of any suspicion that has come to their attention. All the iSTR are logged with the relevant supporting documents/evidence of suspicion.

The Company has designed an iSTR form (Annexure 7), which every team member of the Company can use to report the MLRO for any suspicious. the Company's team members can also inform the MLRO about any suspicious by phone or email.

The key indicators/red flags of suspicious activities include reasonable ground of suspicion that any service or transactions may be:

a. related to criminal conduct;

b. related to the laundering of money or the proceeds of any crime;

c. funds linked or related to, or to be used for, terrorist financing or by proscribed organisations, whether or not the funds represent the proceeds of crime; or

d. made in circumstances of unusual or unjustified complexity;

e. appear to have no economic justification or lawful objective; and

f. give rise to suspicion as per Annex VII (Indicators of Potentially Suspicious transaction /Activity) of AML Code and Section 5 of Guidance Note 3 issued by FIU (Specific Examples of Indicators of Suspicious Transactions).

6.3 STR;

The Company has implemented the control of the Customer profiling and transactional monitoring, therefore any possible alerts are reported to MLRO.

Under the FIAML Act 2002, the Suspicious Transaction Report (STR) means 'a transaction which;

a. Gives rise to a reasonable suspicion that it may involve:

    1. The laundering of money or the proceeds of any crime; or

    2. Funds linked or related to, or to be used for, terrorist financing or by proscribed organizations, 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.

All the suspicious cases which are reported through iSTR, or identified independently from the MLRO, are reviewed and investigated in depth, taking into consideration the provisions of Section 6.5 of the AML Code, and any evidenced suspicion is reported by the MLRO to the FIU in prescribed from of STR as given in http://www.fiumauritius.org/English/Reporting/Pages/default.aspx

Where a Client is declared as a designated party or listed as a listed party under the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019, the Company will immediately, verify the details of the designated party or listed party, and also identify whether the Client owns any funds or other assets in Mauritius.

After identification of the Assets, the Company will make a report to the National Sanctions Secretariat as obligated, and any other Local Authority or Regulator as applicable.

Further to the proclamation of the Anti-Money Laundering and Combating the Financing of Terrorism (Miscellaneous Provisions) Act 2020, emphasis has been put on the obligation to report suspicious transactions, causing amongst others, the FIAMLA 2002 to be amended. Thus, the delay for the Money Laundering Reporting Officer (MLRO) or the Deputy MLRO, to report a validated Suspicious Transaction Report (STR) shall now onwards be 5 working days instead of 15 days from the date on which the suspicion was raised;

Regarding the financial sanctions to the qualifying offences under FIAMLA shall upon conviction be as follows:

- Failure to report a suspicious transaction not later than 5 working days from the date the suspicion was rose – A fine not exceeding MUR 1 million and a term of imprisonment not exceeding 5 years;

- Failure to apply an effective risk assessment in view of detecting an act of money laundering and terrorism financing – A fine not exceeding MUR 10 million and a term of imprisonment not exceeding 5 years;

- Conspiring or assisting in a claimed financial malpractice – A fine not exceeding MUR 10 million and a term of imprisonment not exceeding 5 years;
- Causing obstruction by destroying evidence and relevant records – A fine not exceeding MUR 10 million and a term of imprisonment not exceeding 5 years;
- Objection or failure to provide such requested information to the regulatory body – A fine not exceeding MUR 1 million and a term of imprisonment not exceeding 5 years;

6.4 Tipping Off;

a. Tipping off is prohibited under the provision of Section 19 (1)(c) of the FIAMLA 2002;

b. Since it is an offence based, the MLRO ensures that the management and employees are aware of and are sensitive to the data sharing, and consequences of tipping off;

c. In case the officer and/or employee believes, or has reasonable grounds to believe, that a Customer may be tipped off by conducting CDD measures or on-going monitoring, the employee should refer the case to MLRO. The MLRO shall maintain records to demonstrate the grounds for belief that conducting CDD measures or ongoing monitoring would have tipped off the Customer;

d. If an internal STR is sent to the MLRO, the employee should not disclose this to the Customer or any other person;

e. The MLRO should not accord permission or consent to disclosure of information relating to internal STR to any person, unless MLRO is satisfied that such disclosure would not constitute tipping off;

f. Any letters, notices, or requests received from FIU, or Police these should not be disclosed to any person outside the Compliance Team or Customer;

g. The only permitted exception, apart from disclosures to the FIU and Police, are disclosures to;

    1. an officer or employee or agent of the reporting entity for any purposes connected with the performance of that person's duties;

    2. a legal practitioner, attorney, or legal adviser for the purpose of obtaining legal advice or representation in relation to the matter; and

    3. the supervisory authority of the reporting entity for the purpose of carrying out the supervisory authority's functions.

h. The MLRO should ensure that all officers and employees need to understand that they could be personally liable for non-compliance with the AML obligations; and

i. The MLRO is the person responsible for relevant training in identifying AML suspicious transaction for all officers and employees.

6.5 Records of suspicious transaction reports;

a. MLRO will maintain the following records on suspicious reports:

    1. Internal Disclosure Forms received by the MLRO;

2. Internal suspicious transaction reports and suspicious transactions reports made to the FIU;
3. Where no suspicious report that has been made to the FIU, record of information or material that was considered and the evaluation report mentioning the reason for the decision will be retained.

These records should be retained for the duration of the client relationship and all records should be retained for a period of at least 7 years after the completion of the transaction to which they relate.

7. Training

the Company is committed to the training and development of its board, officers and employees. Regular training ensure that all staff stay aware of their responsibilities in respect of prevention of money laundering including the application of adequate controls, understanding what might constitute suspicious behavior and how to report an such suspicions.

The Compliance Department will be responsible for providing support and assistance in this regard, and for ensuring that training is implemented and documented. Training includes, formal training courses, communication that serves to educate and inform employees, such as emails, newsletters, guidance notes, periodic team meetings and anything else that facilitates the sharing of information.

7.1 Responsibility of Compliance Department:

a. compliance training of officers and employees;

b. customise and continuous training are carried out to suit the Company talent requirements;

c. all employees have an understanding of the fundamental knowledge required to carry out their responsibilities and meet the Company's obligations;

d. Compliance staffs are subject matter experts and will be provided with additional specialised learning opportunities; and

e. Attendance by all officers and employees to such training is mandatory, a record of which will be maintained.

7.2 Anti-Money Laundering training will as a minimum comprise the following issues

a. The need to obtain sufficient evidence of identity;

b. Recognition and reporting of suspicions of money laundering via the MLRO to the FIU; The identity and responsibilities of the MLRO;

c. Anti-money laundering rules, guidance and regulations; and,

d. Effects of breaches of money laundering legislation on the Company and its employees

8. On-Going Enterprise Risk Assessment

As part of its AML/CTF obligations under the laws and regulations, the Company requires its CO and MRLO to produce an annual report to ensure the firm's systems and controls are proportionate to the size, nature and complexity of the operations and remain effective at all times.

8.1 The report includes an assessment and evaluation of:

a. the adequacy of management information systems in place to deliver the information required by the senior management to ensure compliance with their responsibilities;

b. the Company operation and effectiveness of its anti-money laundering systems and controls;

c. appropriate coverage of new products and services, material changes in new customers take on procedures, impact of new regulatory changes in business profile;

d. the way in which new national and international findings have been used during the year.

8.2 The report shall also provide detail on:

a. the number of reports made by staff to the MLRO, dealing separately, if appropriate, with different parts of the firm's business;

b. documentation of risk management policies and risk profiles;

c. monitoring arrangements to ensure that all areas adequately covered.

9. Registers at Compliance Department

The following registers are held at the Compliance department:

a. PEP Register

- Details of Politically Exposed Persons (if any).

b. Suspicious Transaction Report Register

- Details of all the internal suspicious transactions which have been reported to the MLRO/DMLRO.
- Records of actions taken under the internal and external reporting requirements.
- When the MLRO has considered information or other material concerning the reports but has not made a disclosure of suspicion to the FIU, a record of the information or material that was considered and the reason for the decision.
- All reports made by the MLRO to the FIU.

c. AML/CFT Training Register

- Details on the nature of the training, including details of contents and mode of delivery.
- Dates AML/CFT training was provided.
- Names of the employees who received training.

10. Record Keeping

The objective of record keeping is to ensure that the Company can provide necessary information about Customers, and their transactions details at any given time or as per the request for FSC, FIU, Law Enforcement Agencies, Courts, Auditors/Examiners, or any competent authorities. Pursuant to Section 17(b) of FIAMLA 2002 requires the Company to maintain records failure to comply is regarded very seriously by the FIU and may result in regulatory and/or criminal sanctions.

All records will be kept for a minimum period of seven (7) years from the date of the relevant event or, in the case of an ongoing business relationship, after the business relationship ceases, in a form which is immediately accessible upon request.

10.1 Format and Retrieval of Records

a. By way of original hard copy documents;
b. By way of Photocopies (In some case True certified copies) of original documents;
c. In scanned form; and
d. In computerized or electronic form.

10.2 Types of records to be retained;

a. Customer Due Diligence Information:

   Records of Customer Due Diligence related including any investigation and resolution of Red Flag situations are to be retained after on boarding or the relationship ends.

b. Transactions:

   All transaction records will be sufficiently detailed to enable the transaction to be readily reconstructed at any time by the FIU or FSC.
   Transaction records are records containing information on individual transactions, such as;

   1. the name and address of the customer, beneficial owner and underlying principal;
   2. if a monetary transaction, the currency and amount of the transaction;
   3. source and destination of funds including full remitter details (instructions, forms of authority)
   4. account name and number or other information by which it can be identified;
   5. details of the counterparty, including account details;
   6. sale and purchase agreements as well as service agreements;

c. Third Party;

   If the Company has appointed an representative, white label, Introducer, then it is the Company's responsibility to ensure retains all related records.

d. Refused business records;

   Where business has been refused because it does not meet our client identification, verification and KYC standards, a record of the refusal will be retained for 7years.

e. Records of FIU interactions:

Maintaining the records of all AML/CFT enquiries received from the FIU and all reports made to the FIU under s 10 of the AML Act (including STRs and responses to information requests).

f. Internal and external reports:

A record of all internal and external reports relating to suspicions on money laundering activities, together with associated correspondence and supporting evidence will be retained by the Internal Audit Team. Also records of actions taken following the internal and external reporting procedures (including copies of all Suspicious Activity Reports) must be retained for 7 years after the report was made.

g. Reports made by the internal audit team:

These reports to senior management and all actions taken consequently are also to be retained.

h. Training:

Records of training delivered including the date the training was delivered, the nature of the training and the names of the officers and employees trained are all held on file and the records retained for a minimum of 7 years.

i. Correspondence with FSC, MRA, Management Company and other regulatory authorities

j. Compliance Monitoring

Records to ascertain that compliance is being monitored at all levels, record of policies, procedures and controls which are in place, the records must include;

1. Reports by the MLRO to the Board and senior management
2. Records of consideration of those reports and of any action taken as a consequence; and
3. Any records made within the Company.

10.3 Record Retention

The records shall be retained in a medium that allows the storage of information in a way accessible for future reference by the competent authority, and in such a form and manner that the following conditions are met:

1. the competent authority is able to access them readily;
2. it is possible for any corrections or other amendments, and the contents of the records prior to such corrections or amendments, to be easily ascertained;
3. it is not possible for the records otherwise to be manipulated or altered;
4. the Company's arrangements comply with the record keeping requirements irrespective of the technology used; and
5. The Company shall retain records according to Record Retention and Archival Policy.

11. Oversight

a. the Company’s senior management is dedicated to overseeing the AML/CTF program and have ultimate responsibility for ensure compliance. Responsibility for ensuring policies and procedures

are carried out in a manner to comply with AML/CTF laws and regulations is delegated to the firm's Compliance Officer, Money Laundering Reporting Officer and Deputy Money Laundering Reporting Officer.

b. This Manual has been adopted by the Board. Any amendment to this Manual is subject to Board oversight and approval (i.e. the Board must formally adopt any amendment to the Manual

c. AML/CTF is a standing item on the Compliance Committee agenda. Compliance Committee Meetings take place as and when required.

12. ANNEXURE 1: Customer due Diligence Documents

List A: Due Diligence Check List – Individual

Certified copies of documents required on the Individual
(Ultimate Beneficial Owner//Director/Authorised Person):

a. Current valid passport; national identity card; or driving licence;

b. Proof of address in the form of recent utility bill or credit card statement; (all these documents should not be more than 3 months old);

c. Declaration of source of funds

d. Self-Certification From – FATCA/CRS

List B: Due Diligence Check List – Corporate

Certified copies of documents required on the Company

a. Memorandum and Articles of Incorporation of the applicant;

b. Certificate of Incorporation;

c. Applicant business "Financial Services License" / "Business License";

d. Original certificate of Good Standing;

e. Details of the registered office and place of business;

f. Copy of latest audited accounts;

g. List of Directors;

h. Structural chart of the company;

i. Complete set of documents under List A on controlling shareholders (i.e. holding 10% or more of the voting power directly or indirectly of the applicant for business)

j. Certified board resolution authorising the person who acts on its behalf (for corporate shareholder only); and

k. Self-certification form – FATCA/CRS.

List C: Due Diligence Check List – Trust

a. Certified true copy of the extract of the trust deed;

b. Certificate of registration, where applicable;

c. Details of registered office and place of business of the trustee;

d. Complete set of documents on principals of the trust (Trustee, Beneficiaries, Settlor, Protector) as above for individual or company; and

e. Self-Certification form – FATCA/CRS

List D: Due Diligence Check List – Partnership

a. Certified true copy of the partnership deed;
b. Complete set of documents under List A on the manager and the significant partners owning 10% or more of the applicant for business;
c. Copy of the latest report and accounts;
d. Confirmation of the nature of the business of the partnership to ensure that it is legitimate;
e. Certified partner resolution authorising the person who acts on its behalf (for shareholder only);and
f. Self-Certification – FATCA/CRS.

13. ANNEXURE 2: Source of Funds Form

Source of funds and Wealth Declaration and Identity Check of beneficial Owner

Company Name:	
Verification Beneficial Owner	
Full Name / Legal Name:	
Identity No/ Company No:	
Nationality/Country of Incorporation:	
Date of Birth /Date of Incorporation:	
Permanent Residential/ Business Address:	
Telephone No:	
Email:	

I/We hereby confirm that deposits made into the Company:

1. Are not made on behalf of a third party; and
2. The funds deposited are derived from legitimate source and are not linked and/or derived from criminal origin, of whatsoever nature, and in particular do not constitute the proceeds of Money Laundering and Terrorist Financing.

Source of Funds Declaration - Full description of source of funds to be deposited.

Source of Funds: (Check "✓" all that apply)

1. Capital of Company ☐
2. Dividends ☐
3. Income from Business operations ☐
4. Gift ☐
5. Inheritance ☐
6. Profit from sale or maturing Investments ☐
7. Profit from Property sale ☐
8. Income from Sale of Company shares ☐
9. Fixed Deposit Savings ☐
10. Other, (please specify) ☐

Name of remitting bank:
Address of remitting bank:
Remitter Account Name:
Remitter Account Number:
Other details:

Origin of Wealth

Origin of Wealth: (Check "✓" all that apply)

1. Income from Salary ☐
2. Maturity or surrender of Life Insurance Policy ☐

3.	Sale/Liquidation of Investment □
4.	Sale of Property □
5.	Company Sale □
6.	Inheritance □
7.	Divorce Settlement or any other form of settlement compensation □
8.	Company profits □
9.	Retirement Income
10.	Dividend/Royalties Payment □
11.	Employment □
12.	Rental Income □

Acknowledgment and Certification

I/We acknowledge that it is the policy of the Company International Limited to verify the source of funds deposited into the Client Segregated Account and hereby certify that the funds deposited are derived from the sources above.

I/We will provide the required evidence of the source of funds on funds deposited now and/or otherwise required to doing so in future.

I/We further confirm that the transfer of asset to the Company International Limited are not in breach of any money laundering regulations and laws applicable to the Republic of Mauritius, including but not limited to the Financial Intelligence and Anti-Money laundering Act 2002 and 2018, the Prevention of Corruption Act 2002 and the Prevention of Terrorism Act 2002.

DONE IN GOOD FAITH AND AFTER DUE CONSIDERATION.

Full Name	
Authorised Person (if applicable)	
Capacity	
Signature	

14. ANNEXURE 3: Risk Factors Examples and Risk Scoring

The below risk areas and factors are for consideration/guidance.

RISK AREA	RISK FACTORS	ASSOCIATED RISK(S)	RISK SCORING
Client Risk			
The client's and the client's beneficial owner's business or professional activity	Client or beneficial owner have links to following sectors: • construction, • narcotics, pharmaceuticals and healthcare, • the arms trade and defence, • public procurement	Sectors that are commonly associated with **higher** corruption risk	**3-5**
	Client or beneficial owner have links to following cash-intensive sectors: • Money Exchangers/Money services businesses/crowd funding platforms and virtual currencies. • Casinos / internet gambling and other gambling related activities.	Sectors that are associated with **higher** ML/TF risk are money exchanges, casions etc..	**4-5**
	Client is a non-profit organisation	Such activities could be abused for terrorist financing purposes hence carry a **higher** TF risk	**4-5**
	Client is a Politically Exposed Person (PEP). Beneficial owner/family member is a PEP or persons known to be close associates of PEP. The client or beneficial owner have other relevant links to a PEP, for example, the client's directors are PEPs and, if so, these PEPs exercise significant control over the client or beneficial owner.	Involves the **highest** level of corruption risk	**5** PEP client is always High Risk, regardless of the overall score

Client's or beneficial owners' reputation	Adverse media reports or other relevant sources of information about the client, for example allegations of criminality or **terrorism** against the client or the beneficial owner.	Potential risk of involvement in illegal activities, as absence of criminal convictions alone may not be sufficient to dismiss allegations of wrongdoing which is associated to **higher** levels or risk.	**3-5**
	Client, beneficial owner or anyone publicly known to be closely associated with them had their assets frozen due to administrative or criminal proceedings or allegations of terrorism or terrorist financing.	Risk of placement of previously earned illegal proceeds into the financial system which is associated to **higher** levels or risk.	**3-5**
	The firm knows that the client or beneficial owner has been the subject of a suspicious transactions report in the past.	Risk of placement of previously earned illegal proceeds into the financial system	**3-5**
	The Client or beneficial owner is listed or related to the Sanction List, however requests services which are not restricted by such sanction.	Risk of illegal activities	**3-5**
	The Client or beneficial owner and/or their affiliates are listed in the Panama papers, or other offshore leaks.	Risk of illegal activities	**3-5**
Client's or beneficial owner's nature and behaviour			
	The Client is a Trust/ Fund	Risk of hiding the identity of the controlling persons could give rise to **higher** ML/TF Risk.	**3-5**
	The firm has doubts about the veracity or accuracy of the client's or beneficial owner's identity.	False identity might be a sign of criminal activity which can lead to **higher** ML/TF risks.	**4-5**
	The Client's ownership and control structure is complex (set number of levels e.g. 3 levels).	Complex structure might be a sign of criminal activity , tax	**1-5**

		evasion or other actions which can lead to **higher** ML/TF risks.	
	The client has nominee shareholders or shares in bearer form.	Hiding the UBO might be a sign of criminal activity, tax evasion or other actions which can lead to **higher** ML/TF risks.	**1-5**
	The business relationship is conducted in unusual circumstances, for example the customer is reluctant to share CDD information or appears to want to disguise the true nature of the business relationship.	Hiding of information might be a sign of criminal activity, tax evasion or other actions which can lead to ML/TF risk. Hiding information might mean that the identity of the real beneficiary is not disclosed/identified which leads to **higher** level of risk.	**3-5**
	The client requests unnecessary or unreasonable levels of secrecy, for example, reluctant to share CDD information, or appear to want to disguise the true nature of their business.	Hiding of information might be a sign of criminal activity, tax evasion or other actions which can lead to **higher** ML/TF risk.	**3-5**
Transaction Risk			
Deposit and withdrawal of funds	• Client deposited funds into the trading account and requested repayment of funds within a short period of time with ni apparent reason; • Transferring of funds through several accounts; • Little or no trading was recorded during the period; and • The amount of funds deposited was not in line with the client's profile.	Use of Margin Account with Littel trading can lead to **higher** ML/TF risk	**3-5**

Deposits by currency exchanges	FX dealer or bureau de exchange orders the transfers	Use of foreign exchange dealer can lead to **higher** ML/TF risk	**3-5**
Geographical Risk			
Countries and geographical areas risk factors	The Clients or the client's beneficial owner is based and/or has business activities: • locally or in the EU • third countries with an effective AML/CFT system • third countries with low level of corruption of other criminal activity (credible source)	Jurisdictions associated to moderate levels of risk	**1-3**
	The Client or client's beneficial owner is based and/or has business activities and/or has funds in a jurisdiction associated with: • high ML/TF Risk or is subject to sanctions/embargoes e.g. UN, EU. • inadequate AML/CTF systems e.g. EU high-risk third country lists • having significant levels of corruption or other criminal activities such as narcotics, arm dealing, human trafficking, illicit diamond trading, etc • terrorist activities or have designated terrorist organizations operating within their country.	Represent Highest ML/TF Risk.	**5**
Delivery Channel Business Risk			
Delivery Channel Business Risk	The Client is having been introduced by 3rd Party	The 3rd party on which reliance is placed, may not apply due diligence.	**3-5**

15. ANNEXURE 4: Risk Assessment Table

RISK PROFILING TABLE of VT MARKETS LIMITED

Name of client: Login Number:

	A. Client Details •	
1	**Type of client** I. Individual/Corporate (with trading experience) - 5% II. Individual/Corporate (without trading experience) -10%	
2	**Client: New (5%) or Existing (3%)**	
3	**Location of client** I. Equivalent Jurisdiction - Low (3%) II. Non- Equivalent Jurisdiction- Medium (7%) or High (10%) III. Unknown (10%)	
	Source of funds I. Equivalent Jurisdiction - Low (3%) II. Non- Equivalent Jurisdiction - Medium (7%) or High (10%) III. Unknown (10%) **Source of Initial funds** Check by Credentia International Management Ltd: I. Name of client II. Country of location III. Amount of Initial funds IV. Source of Funds	
B.	**Customer Due Diligence**	
1	**All CDD documents** (Partial – 15%; Complete – 0%)	
2	**All EDD documents (if applicable) – 15%**	
3.	**i. PEP (15%)** **ii. Non – Pep (0%)**	
C.	**Product Risk** Securities/Shares/CFD (10%) Currency Pairs (15%)	

D.	**Deposit Channel** Wire Transfer (5%) Payment Gateways (10%)	
	Frequency of Deposit (5%)	
	Amount above 14K (5%)	
E.	**Sanction List** - IOSCO Investors Alert List ☐ - UNSR Sanction List ☐ - Source: https://www.knowyourcountry.com/country-ratings-table ☐ - Source: ☐ http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations	
	TOTAL: |	
Prepared By: Approved By: Signature: Date:		

16. ANNEXURE 5: Ongoing Customer Review Form

Review date:

Customer Name:

Type of Customer:

Corporate Account □

Personal Account □

Information on Customer

1. **Name of Customer:**
   a. Remain unchanged □
   b. Changed □

2. **Status of Account:**
   a. Active □
   b. Blocked □
   c. Dormant □

3. **PEP Status:**
   a. Yes, date of verification □
   b. No, date of verification □
   c. PEP Status found to:
   d. Former PEP Status found to:

4. **Customer's Data:**
   a. **Non-cash transactions (monthly amount of turnover):**

      □ Remain unchanged

      □ Reduced to the amount

      □ Increased to the amount

   b. **Regions/Countries of Customer's activity:**

      □ High ML/TF countries

      □ Does not pose high ML/TF risk

      Submitted Yes □ No □

   c. **Business Address:**

      □ Remain unchanged

      □ Changed (pls specify)

   d. **Main Business Activity:**

      □ Remain unchanged

      □ Expanded

      □ High ML/TF risk business activity

      □ Business Activity does not pose high ML/TF risk

      □ Narrowed

5. **Inquiries from supervising authorities, FIU, internal evaluations/reports/due diligence during business relationship**
   a. **FIU**

Yes □

No □

b. FSC

Yes □

No □

6. Structure of the Company:

a. UBO

Remain unchanged □

Changed (pls specify) □

b. Authorized person:

Remain unchanged □

Changed (pls specify) □

c. Director

Remain unchanged □

Changed (pls specify) □

d. Shareholder

Remain unchanged □

Changed (pls specify) □

e. Beneficial owner

1. Name and Surname

Remain unchanged □

Changed (pls specify) □

2. Identification details

Remain unchanged □

Changed (pls specify) □

3. Permanent residential address

Remain unchanged □

Changed (pls specify) □

f. Authorized person:

1. Name and Surname

Remain unchanged □

Changed (pls specify) □

2. Identification details

Remain unchanged □

Changed (pls specify) □

3. **Permanent residential address**

Remain unchanged □

Changed (pls specify) □

g. Director

1. **Name and Surname**

Remain unchanged □

Changed (pls specify) □

2. **Identification details**

Remain unchanged □

Changed (pls specify) □

3. **Permanent residential address**

Remain unchanged □

Changed (pls specify) □

h. Shareholder

1. **Name and Surname**

Remain unchanged □

Changed (pls specify) □

2. **Identification details**

Remain unchanged □

Changed (pls specify) □

3. **Permanent residential address**

Remain unchanged □

Changed (pls specify) □

CONCLUSION OF COMPLIANCE OFFICER

A. Specify your conclusions and mention the information/documents required from the Customer, deadline for submission

□ Business relationship to be continued

□ Business Relationship to be terminated

B. ML/TF risk profile of the Customer

□ LOW (Specify)

□ MEDIUM

□ HIGH (specify risk increasing factor/factors)

□ HIGH PEP (Specify)

Management Approval obtained

Yes □

No □

Prepared by:

Name:

Position:

Date:

17. ANNEXURE 6: Some Examples of Red Flags

1. Customers who wish to maintain several trustee or client accounts that do not appear consistent with the type of business, including transactions involving nominee names
2. Matching withdrawals with deposits by different ways on the same or previous day.
3. Exposure or abuse of transfers without completing trading operations on the trading account.
4. Revelation of unusual nature of operations that do not have obvious economic substance or obvious legal purpose.
5. Customers who give conflicting information to different staff members.
6. A customer exhibits an unusual level of concern for secrecy, particularly with regard to the customer's identity, type of business or source of assets.
7. Revelation of circumstances implying that the operations are performed for the purpose of money laundering or financing terrorism.

18. ANNEXURE 7: Internal Suspicious Transactions Report (iSTR)

Internal Disclosure Form to MLRO

1. Reporting Employee;

Name:

Telephone No:

2. Customer Details;

Client Name:

Address:

Contact Name:

Contact Telephone No:

Date Business Relationship Commenced:

Customer reference:

3. Information/Suspicion

Suspected Information/Transaction:

Reasons for Suspicion:

Please attach copies of any relevant documentation to this report.

Reporter's Signature: Date:

It is an offence to advise the Customer or anyone else of your suspicion and report. This report will be treated in the strictest confidence.

For MLRO Use:

Date received: …….. Time received: ……Ref:…….

FIU advised …. Yes/No Date: …….. Ref:

19. ANNEXURE 8: Source of Wealth and Fund Examples

List of examples of appropriate information and/or supporting documentation required to establish Source of Wealth and Funds:

Source of funds/Wealth	Information / Documents that may be required
Savings/Deposits	• Bank statement and enquiry of the source of wealth.
Loan	• Loan agreement. • Amount, date and purpose of loan. • Name and address of Lender. • Details of any security.
Company Sale	• Copy of the contract of sale. • Internet research of Company Registry. • Name and Address of Company. • Total sales price. • Customer's share participation. • Nature of business. • Date of sale and receipt of funds – Media coverage.
Company Profits / Dividends	• Copy of latest audited financial statements. • Copy of latest management accounts. • Board of Directors approval. • Dividend distribution. • Tax declaration form.
Other income sources	• Nature of income, amount, date received and from whom. • Appropriate supporting documentation

20. ANNEXURE 9: FATCA/CRS Declaration

FATCA Compliance

The Foreign Account Tax Compliance Act (FATCA) is a United States federal law that requires United States persons, including individuals who live outside the United States, to report their financial accounts held outside of the United States, and requires foreign financial institutions to report to the Internal Revenue Service (IRS) about their U.S. clients. This form has been designated with regards of Foreign Account Tax Compliance Act FATCA to capture the citizenship and residence for Tax Purposes of the person entitled to the income and assets associated with an account (the beneficial owner).

		Yes	No	Remarks
1.	Is the applicant a United States (U.S) Citizen or Lawful Permanent Resident?			If *yes*, please provide **Form W-9.**
2.	Is the applicant born in U.S?			If *yes*, please provide **Form W-9** or **W-8 BEN**; and a **Non-US passport** establishing foreign citizenship.
3.	Is the Power of Attorney or signatory authority granted to a person with a U.S address?			If *yes*, please provide **Form W-9** or **W-8 BEN**; and a **Non-US passport** establishing foreign citizenship.
4.	Will there be instructions to transfer funds to U.S accounts or directions regularly received from a U.S address?			If *yes*, please provide **Form W-9** or **W-8 BEN**; and **documentary evidence** establishing non U.S state.
5.	Will there be address on file which is "in care of" or "hold mail" in U.S or U.S P.O Box and/or a U.S telephone number?			If *yes*, please provide **Form W-9** or **W-8 BEN**; and **documentary evidence** establishing non U.S state.

I/We hereby certify that the information above is correct, true and complete and agree to inform Agenius Management Services Limited of any change in the information provided

Date	
Name in Full	
Signature	

21. ANNEXURE 10: Politically Exposed Person Self-Declaration Form

As part of its due diligence procedures we require certain individuals to make a formal declaration as to whether or not they would be considered a Politically Exposed Person (PEP) as defined under the Mauritius Law.

A PEP is defined as a person who holds, or has held at any time in the last year;

1. A prominent public function, including:
    a) Heads of State, Heads of Government, Ministers and Deputy and Assistant Ministers and Parliamentary Secretaries;
    b) Members of Parliament;
    c) Members of the Courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
    d) Members of courts of auditors, Audit Committees or of the boards of central banks;
    e) Ambassadors, charge d'affaires and other high-ranking officers in the armed forces;
    For the purposes of (a) to (e) above this includes positions held at the Community or international level

2. Members of the administration, management or boards of State-owned corporations.

PEP Family Members & Close Associate

The legislation extends the definition of PEPs to immediate family members and close associates of PEPs.

1. An immediate family member includes any of the following:

a) the spouse, or any partner recognised by national law as equivalent to the spouse;
b) the children and their spouses or partners; and
c) the parents

2. A close associate is defined to include any of the following persons:

a) an individual who has joint beneficial ownership of a body corporate or any other form of legal arrangement or any other close business relations with a PEP; or
b) an individual who has sole beneficial ownership of a body corporate or any other form of legal arrangement that is known to have been established for the benefit of a PEP.

Having read and understood the above definition I confirm and declare that: (please select accordingly)

I am NOT a Politically Exposed Person (PEP) ☐

I am a Politically Exposed Person (PEP) ☐

I hereby declare that the declaration provided above is true and correct.

Name (in blocks): _____

Signature: _____

Date: _____

22. ANNEXURE 11: Glossary

Glossary

AML Code	FSC Code on the Prevention of Money Laundering and Terrorist Financing
Applicant for Business	Includes any natural or legal person or arrangement – whether corporate or unincorporated – that seeks to form a business relationship or to carry out a one-off transaction with a license.
Beneficial Owner	the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement;
Business relationship	an arrangement between an applicant for business and a Licensee where the purpose or effect of the arrangement is to facilitate the carrying out of transactions between the applicant for business and the Licensee on a frequent, habitual or regular basis;
Controller	has the same meaning as in the FS Act
CDD	means customer due diligence
CFT	Combating the Financing of Terrorism;
Equivalent jurisdiction	A jurisdiction which has in place anti-money laundering legislation that is at least equivalent to the anti-money laundering legislation in Mauritius. See Appendix VI of AML Code.;
Money Laundering Reporting officer	Means an officer appointed pursuant to regulations 6(1)(a) Financial Intelligence and Anti-Money Laundering Regulations 2003
FATF	Means the intergovernmental body know as Financial Action Task Force;
FIAMLA	Financial Intelligence and Anti-Money Laundering Act 2002 and 2018;
Financial Intelligence "FIU"	Means the financial intelligence unit;
FSC	Financial Services Commission Mauritius;
FS Act	Financial Services ACT 2007;
Shell Banks	Means a bank that has no physical presence in the country in which it is incorporated and licensed, and which. is unaffiliated with a regulated financial group that is subject to effective consolidated supervision.

23. ANNEXURE 12: Anti-Money Laundering & Compliance Manual Declaration

a. I hereby acknowledge that I have read and understood the provisions of the Company's Anti- Money Laundering & Compliance Manual ("Manual").

b. I agree to comply with the policies and procedures of the Manual. If I am ever unsure about any of the areas covered in this Manual, I will consult the Company's Compliance officer and Money Laundering Reporting Officer.

c. I understand that a breach of any of the provisions of the Manual may result in criminal prosecution, regulatory censure or disciplinary action by the Company.

Name:

Signature:

Date:

24. ANNEXURE 13: List of Banned Countries

Below is a list of countries that are considered banned in which the Company is unavailable;

Afghanistan
Albania
American Samoa
Belarus
Bermuda
Bosnia And Herzegovina
Burundi
Canada
Central African Republic
China
Cuba
Democratic Republic of Congo
Eritrea
Guam
Guinea
Guinea-Bissau
Haiti
Iran
Iraq
Lebanon
Liberia
Libya
Mali
Myanmar
Nicaragua
North Korea
Northern Mariana Islands
Puerto Rico
Romania
Russia
Sierra Leone
Singapore
Somalia
South Sudan
Sudan
Syria
Tunisia
Ukraine
United States of America
Venezuela
Virgin Islands, US
Yemen
Zimbabwe