



ANTI- MONEY LAUNDERING & COMBATING TERRORISM FINANCING MANUAL

VERSION CONTROL

Owner	Compliance Officer
Version	5.0
Status	Final
Approved by	Board of Directors
Date of last review	29/05/2026

Approved by Board of Directors

Signature



Date 01.06.2026

This Anti- Money Laundering & Combating Terrorism Financing Manual ("Manual") is to be strictly adhered to by all employees. Non-compliance with this Manual by any employee shall result in disciplinary actions. There are no exceptions to the Manual without the prior written approval of the Compliance Officer and the Managing Director. Any questions, comments or concerns regarding to the Manual should be directed to the Compliance Officer.



1. INTRODUCTION

This Anti- Money Laundering & Combating Terrorism Financing Manual (“Manual”) represents the basic standards of Anti-Money Laundering and Combating Terrorism Financing (hereinafter collectively referred to as AML) procedures of Octrado Ltd. (the “Company”). The Company drafted its Manual in compliance with all applicable laws and regulations with respect to AML.

The Manual is developed and periodically updated by the Money Laundering Compliance Officer (“MLCO”) based on the general principles set up by the Company’s Board of Directors (“BoD”) in relation to the AML prevention.

The Manual shall be communicated by the MLCO to all the employees of the Company that manage, monitor or control in any way the clients’ transactions and have the responsibility for the application of the practices, measures, procedures and controls that have been determined herein.

All amendments and/or changes of the Manual must be approved by the BoD.

2. THE RESPONSIBILITIES OF THE BOARD OF DIRECTORS

The responsibilities of the BoD in relation to the AML prevention include the following:

- to determine, record and approve the general policy principles of the Company in relation to the AML prevention and to communicate them to MLCO;
- to appoint a senior official that possesses the skills, knowledge and expertise relevant to financial and other activities depending on the situation, who shall act as MLCO and, where is necessary, assistant MLCO and determine their duties and responsibilities, which are recorded in this Manual. Only persons who shall possess the relevant approval from the regulator shall be appointed as the MLCO, unless an exception has been obtained from the regulator;
- to approve the Manual;
- to ensure that all requirements of the laws and regulations are applied, and assure that appropriate, effective and sufficient systems and controls are introduced for achieving the abovementioned requirement;
- to ensure that the Compliance Officer and any other person who have been assigned with the duty of implementing the procedures for the AML prevention, have complete and timely access to all data and information concerning clients' identity, transaction documents (as and where applicable) and other relevant files and information maintained by the Company so as to be fully facilitated in the effective execution of their duties, as included herein;
- to ensure that all employees are aware of the person who has been assigned the duties of the MLCO, to whom they report, any information concerning transactions and activities for which they have knowledge or suspicion that might be related to AML;
- to establish a clear and quick reporting chain based on which information regarding suspicious transactions is passed without delay to the MLCO;
- to ensure that the MLCO has sufficient resources, including competent staff and technological equipment, for the effective discharge of their duties;
- to implement adequate and appropriate systems and processes to detect, prevent and deter ML.

3. THE RESPONSIBILITIES OF THE MONEY LAUNDERING COMPLIANCE OFFICER

The MLCO shall belong hierarchically to the higher ranks of the Company's organisational structure so as to command the necessary authority. Furthermore, the MLCO shall lead the Company's AML Procedures and processes and report to the BoD. The MLCO shall also have the recourses, expertise as well as access to all relevant information necessary to perform his duties adequately and efficiently.

The level of remuneration of the MLCO shall not compromise his objectivity. The responsibilities of the MLCO in relation to prevention of AML include following:

- to design, the internal practice, measures, procedures and controls relevant to the AML prevention, and describe and explicitly allocate the appropriateness and the limits of responsibility of each department that is involved in the abovementioned. It is provided that, the above include measures and procedures for the prevention of the abuse of new technologies and systems providing financial services, for the purpose of AML (e.g. services and transactions via the internet or the telephone) as well as measures so that the risk of AML is appropriately considered and managed in the course of daily activities of the Company with regard to the development of new products and possible changes in the Company's economic profile (e.g. penetration into new markets);
- to review and update the Manual as may be required from time to time, and for such updates to be communicated to the BoD for their approval;
- to monitor and assess the correct and effective implementation of the Manual, the practices, measures, procedures and and in general the implementation of the Manual. In this respect the MLRO shall apply appropriate monitoring mechanisms which will provide him/her with all the necessary information for assessing the level of compliance of the departments and employees of the Company with the procedures and controls which are in force. In the event that the MLRO identifies shortcomings and/or weaknesses in the application of the required practices, measures, procedures and controls, gives appropriate guidance for corrective measures and where deems necessary informs the BoD;
- to receive information from the Company's employees which is considered to be knowledge or suspicion of money laundering or terrorist financing activities or might be related with such activities. The information is received in a written report form. This would be either Suspicious Transaction Report or Suspicious Activity Report.
- to evaluate and examine the information received in the Internal Suspicious Report, by reference to other relevant information and discuss the circumstances of the case with the informer and where appropriate, with the informer's superiors. The evaluation of the information of point above shall be done on a report.
- to file Suspicious Transaction Reports ("STR") and Suspicious Activity Reports ("SAR") to the Financial Intelligence Unit ("FIU");
- to detect, record, and evaluate, at least on an annual basis, all risks arising from existing and new clients, new financial instruments and services and update and amend the systems and procedures applied by the Company for the effective management of the aforesaid risks;
- to ensure the preparation and maintenance of the list of clients categorised following a risk based approach, which contains, among others, the names of clients, their account number and the dates of the commencement of the business relationship. Moreover the MLCO ensures the updating of the said list with all new or existing clients, in light of any additional information obtained;
- to detect, record, and evaluate, at least on an annual basis, all risks arising from existing and new clients, new financial instruments and services and update and amend the systems and

- procedures applied by the Company for the effective management of the aforesaid risks
- to provide advice and guidance to the employees of the Company on subjects related to AML;
 - to acquire the knowledge and skills required for the improvement of the appropriate procedures for recognising, preventing and obstructing any transactions and activities that are suspected to be associated with AML;
 - to determine whether the Company's departments and employees that need further training and education for the purpose of preventing AML and organises appropriate training sessions/seminars. In this respect, MLCO prepares and applies an annual staff training program. Also, the MLCO assesses the adequacy of the education and training provided;
 - to prepare correctly and submit timely to quarterly reports;
 - to prepare the Annual Report;
 - to respond to all requests and queries from the regulator.

4. MONEY LAUNDERING

Money laundering is a generic term used to describe any process that conceals the origin or derivation of the proceeds of crime so that the proceeds appear to be derived from a legitimate source. Money laundering is sometimes wrongly regarded as an activity that is associated only with organized crime and drug trafficking. It is not. It occurs whenever any person deals with another person's direct or indirect benefit from crime. The term 'money laundering' is in fact a misnomer. Often it is not money that is being laundered but other forms of property that directly or indirectly represent benefit from crime. Any form of tangible or intangible property is capable of representing another person's benefit from crime.

The main objective of the money launderer is to transform 'dirty' money into seemingly clean money or other assets in a way to leave as little trace as possible of the transformation. The Company shall support regulators such as Financial Action Task Force ("FATF"), Office of Foreign Assets Control ("OFAC"), United Nations ("UN") and the local regulatory authority, namely the Financial Services Authority ("FSA") which collectively set and enforce standards for anti- money laundering and counter terrorist financing policies and programs. Employees will be screened while recruiting with regards to the AML & compliance procedures by MLCO.

Employees shall ensure that they adhere to the standards to comply with norms set forth by local as well as international regulatory authorities and to protect company and its reputation from being misused for any illicit activity.

Traditionally, money laundering has been described as a process that takes place in three stages as follows:

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

Layering – After successfully injecting the illicit funds into the financial system, laundering them requires creating multiple layers of transactions that further separate the funds from their illegal source. The purpose of this stage is to make it more difficult to trace these funds to the illegal source.



Integration – This is the final stage in a complete money laundering operation. It involves reintroducing the illegal funds into the legitimate economy. The funds now appear as clean income. The purpose of the integration of the funds is to allow the criminal to use the funds without raising suspicion that might trigger investigation and pursuit.

In reality, the three stages often overlap and the benefit from many crimes including most financial crimes does not need to be ‘placed’ into the financial system. The Company is most likely to be exposed at the layering and integration stages of the money laundering process.

Money laundering is a crime that is most often associated with banking and money remittance services. Whilst banks are often an essential part of successful laundering schemes, the financial and related services that the Company offers are also vulnerable to abuse by money launderers. The fight against money laundering is an evolving and never ending process. Money laundering not only harms the public as a whole, but it shakes the financial services industry. It is clearly in the best interest of the financial industry to take appropriate actions to prevent money laundering.

5. TERRORIS FINANICNG

Terrorist financing is the act of providing financial support to acts of terror, terrorists or terrorist organizations to enable them to carry out terrorist acts. Unlike other criminal organizations, the primary aim of terrorist groups is non-financial. Yet, as with all organizations, terrorist groups require funds in order to carry out their primary activities.

This simple fact – the need for funds – is key in fighting terrorism. Follow the money. Follow the financial trail. This is the core objective of all measures that aim to identify, trace, and curb terrorist financing.

There are similarities and differences between money laundering and terrorist financing.

Differences include:

- i. Terrorist financing is an activity that supports future illegal acts, whereas money laundering generally occurs after the commission of illegal acts;
- ii. Legitimately derived property is often used to support terrorism, whereas the origin of laundered money is illegitimate;

Similarities include:

- i. Terrorist groups are often engaged in other forms of criminal activity which may in turn fund their activities;
- ii. Both money laundering and terrorist financing require the assistance of the financial sector.

The key to the prevention of both money laundering and terrorist financing is the adoption of adequate Costumer Due Diligence (“CDD”) measures both at the commencement of every relationship and on an on-going basis thereafter.

6. RISK BASED APPROACH

6.1 Principles of Risk Based Approach Framework

The Company shall apply appropriate measures and procedures, by adopting a risk-based approach, so as to focus its effort in those areas where the risk of AML appears to be comparatively higher.

In this respect the MLCO shall monitor and evaluate, on an on-going basis, the effectiveness of the measures and procedures of this Section of the Manual. The adopted risk-based approach that is followed by the Company, and described in the Manual, has the following general characteristics:

- Recognises that the money laundering or terrorist financing threat varies across clients, countries, services and financial instruments;
- Allows the BoD to differentiate between clients of the Company in a way that matches the risk of their particular business;
- Allows the BoD to apply its own approach in the formulation of policies, procedures and controls in response to the Company's particular circumstances and characteristics;
- Helps to produce a more cost-effective system;
- Promotes the prioritisation of effort and actions of the Company in response to the likelihood of AML occurring through the use of the Services the Company is licensed to offer.

The risk-based approach adopted by the Company, and described in the Manual, involves specific measures and procedures in assessing the most cost effective and appropriate way to identify and manage the AML risks faced by the Company.

Such measures include:

- identifying and assessing the AML risks emanating from particular clients or types of clients, financial instruments, services, and geographical areas of operation of its clients;
- managing and mitigating the assessed risks by the application of appropriate and effective measures, procedures and controls;
- continuous monitoring and improvements in the effective operation of the policies, procedures and controls.

The application of appropriate measures and the nature and extent of the procedures on a risk-based approach depends on different indicators.

Such indicators include the following:

- the scale and complexity of the services offered;
- geographical spread of the services and clients;
- the nature (e.g. non face-to-face) and economic profile of clients as well as of financial instruments and services offered;

- the distribution channels and practices of providing services; the volume and size of transactions;
- the degree of risk associated with each area of services;
- the country of origin and destination of clients' funds;
- deviations from the anticipated level of transactions;
- the nature of business transactions.

The MLRO shall be responsible for the development of the policies, procedures and controls on a risk-based approach. Further, the MLRO shall also be responsible for the implementation of the policies, procedures and controls on a risk-based approach

6.2 Identification of Risks

The risk-based approach adopted by the Company involves the identification, recording and evaluation of the risks that have to be managed. The Company shall assess and evaluate the risks it faces, for the use of the services it is licensed to offer for the purpose of the AML. The particular circumstances of the Company determine suitable procedures and measures that need to be applied to counter and manage risk.

In the cases where the services and the financial instruments that the Company provides are relatively simple, involving relatively few clients or clients with similar characteristics, then the Company shall apply such procedures which are able to focus on those clients who fall outside the 'norm'. The Company shall be, at all times, in a position to demonstrate to regulator that the extent of measures and control procedures it applies are proportionate to the risk it faces for the use of the services, for the purpose of AML.

6.3 Company Risks

The following, *inter alia*, are sources of risks which the Company faces with respect to AML:

- i. *Risks based on the client's nature:*
 - complexity of ownership structure of legal persons;
 - companies incorporated in offshore centres;
 - Politically Exposed Persons ("PEPs");
 - Clients engaged in transactions which involves significant amounts of cash;
 - Clients from high risk countries or countries known for high level of corruption or organised crime or drug trafficking;
 - Clients included in the leaked documents of Mossack Fonseca (Panama Papers);
 - Clients convicted for a predicate offence (and already served their sentence);
 - unwillingness of client to provide information on the Beneficial Owners of a legal person.
- ii. *Risks based on the client's behaviour:*
 - Client transactions where there is no apparent legal financial/commercial rationale;
 - situations where the origin of wealth and/or source of funds cannot be easily verified;
 - unwillingness of clients to provide information on the Beneficial Owners of a legal person.

iii. *Risks based on the client's initial communication with the Company:*

- Non-face-to-face client;
- Clients introduced by third person.

iv. *Risks based on the Company's services and financial instruments:*

- services that allow payments to third
- persons/parties; large cash deposits or withdrawals;
- products or transactions which may favour anonymity.

6.4 Division into Risk Categories

Having performed the risk assessment based on the criteria described above, the MLRO then determines which clients fall into categories of low, medium, high risk or prohibited clients/Unacceptable. All clients are risk rated at the time of "onboarding" and periodically thereafter, depending on the initially attributed risk rating. High risk clients will be subject to additional monitoring and will be red flagged.

The Company uses the following classifications:

- Low Risk;
- Medium Risk;
- High Risk;
- Prohibited Clients/Unacceptable Clients;

6.4.1 Client Categorisation Criteria- LOW RISK CLIENTS

The Company may apply simplified due diligence to the following types of Clients provided that this a low risk or no suspicion for AML.

- When the Company listed companies whose securities are admitted to trading on a regulated market in a country a country which is subject to disclosure requirements consistent with Seychelles legislation;
- Domestic public authority;
- Regulated financial institution.

It is provided that, further to the cases mentioned above, the Company has to gather sufficient information to establish if the client qualifies as a low-risk client. In this respect, the Compliance Officer shall be responsible to gather the said information. The said information shall be duly documented and filed, as applicable, according to the recording keeping procedures.

6.4.2 Client Categorisation Criteria- MEDIUM RISK CLIENTS

The following types of Clients can be classified as medium risk Clients with respect to the AML risk which the Company faces:

- any Client who does not fall under the 'low risk Clients' or 'high risk Clients' categories.

6.4.3 Client Categorisation Criteria- HIGH RISK CLIENTS

The following types of clients can be classified as high risk clients with respect to the AML risk which the Company faces:

- Clients who are not physically present for identification purposes (non face-to-face Clients); trust accounts;
- 'Client accounts' in the name of a third person;
- PEPs' accounts;
- Clients who are involved in electronic gambling/gaming activities through the internet;
- Clients from countries which inadequately apply FATF's recommendations;
- Clients included in the leaked documents of Mossack Fonseca (Panama Papers);
- Clients convicted for a predicate offence (and already served their sentence); cross-frontier correspondent banking relationships with credit institutions-clients from third countries;
- any other clients that their nature entail a higher risk of AML;
- any other Client determined by the Company itself to be classified as such.

6.4.4 Client Categorisation Criteria- PROHIBITED CLIENTS

Prohibited clients include:

- Any client whose name appears on the List of Specially Designated Nationals and Blocked Persons maintained by the U.S. Office of Foreign Assets Control ("OFAC"), which may be found at <http://www.treasury.gov/resource-center/sanctions/Pages/default.aspx>;
- Common Foreign & Security Policy of the European Union, which may be found at http://eeas.europa.eu/cfsp/sanctions/consol-list_en.htm;
- Any client whose name appears on World-Check, which may be found at <http://www.world-check.com>, or equivalent client screening applications; Foreign Shell Banks;
- High-risk clients that have not satisfied the enhanced due diligence requirements;
- Such other lists of prohibited persons and entities as may be mandated by applicable laws or regulations, or maintained internally;
- Nationals of Afghanistan, Cuba, North Korea, Crimea, Israel, Sudan, Bosnia and Herzegovina, Ethiopia, Iran, Iraq, Lao's People Democratic Republic, Syria, Uganda, Vanuatu and Yemen.

6.5 Design and Implementation of Measures and Procedures to Manage and Mitigate the Risks

Taking into consideration the assessed risks, the Company shall determine the type and extent of measures it will adopt in order to manage and mitigate the identified risks in a cost effective manner.

These measures and procedures include:

- adaption of the Client Due Diligence Procedures in respect of clients in line with their

assessed AML risk;

- requiring the quality and extent of required identification data for each type of client to be of a certain standard (e.g. documents from independent and reliable sources, third person information, documentary evidence);
- obtaining additional data and information from the clients, where this is appropriate for the proper and complete understanding of their activities and source of wealth and for the effective management of any increased risk emanating from the particular business relationship or the occasional transaction;
- ongoing monitoring of high risk clients' transactions and activities, as and when applicable.

In this respect, it is the duty of the MLRO to develop and constantly monitor and adjust the Company's policies and procedures with respect to the Client Acceptance Policy and Client Due Diligence and Identification Procedures of the Manual, respectively, as well as via a random sampling exercise as regards existing Clients. These actions shall be duly documented and form part of the Annual Money Laundering Report, as applicable.

6.6 Suspicious Activities

As the types of transactions which may be used by a money launderer are almost unlimited, it is difficult to define a suspicious transaction. Suspicion is personal and subjective and falls far short of proof based on specific evidence. However, it is more than the absence of certainty that someone is innocent. Where there is a business relationship, an unusual or suspicious transaction will often be one which is inconsistent with a client's known legitimate business profile or personal activities or with the normal business for that type of relationship. Therefore the first key to recognition is 'knowing enough' about the client and his/her business to recognise whether a transaction or series of transactions is unusual.

6.6.1 Characteristics to watch for

There are a number of characteristics which are a common feature of money laundering activity. Some of these are:

- Reluctance to provide basic information to verify identity;
 - Engaging in transactions which do not make commercial sense;
 - Transactions out of character with the business expected or with the history of the relationship;
 - Reluctance to clearly explain source of funds;
 - Transfers to/from parties unrelated to the account holder without proper explanation;
 - Multiple similar transactions that could have been more effectively combined;
- transactions spanning many jurisdictions with no obvious reason.

The existence of one or more of the above characteristics does not automatically mean that a client is a money launderer. However, they are an indication that something may be wrong and should give rise to further scrutiny. The client may have a perfectly good reason for the unusual characteristics which would allay any suspicion.

The MLRO shall coordinate a periodic risk based review of the Company's existing clients in order to verify that no client is a Prohibited Client, as defined below, and to ensure the adequacy of the ongoing due

diligence performed on existing clients. The review is performed at least annually or as often as deemed appropriate by the MLRO.

If such a suspicious activity is detected the Company requires of any employee, who detects suspicious activity or has reason to believe that suspicious activity is taking place, to immediately inform the MLRO. Under no circumstances may an employee discuss the suspicious activity, or the fact that it has been referred to the MLRO, with the client concerned. The MLRO shall determine whether to report to appropriate law enforcement officials any suspicious activity of which he/she becomes aware.

6.6.2 Examples of Potentially Suspicious Scenarios

The following are examples of unusual or suspicious transactions, sometimes called “red flags”. Staff should be aware that unusual behaviour could occur at any time during a relationship with a client. The list is not exhaustive, but is provided to assist staff in understanding transactions which could be unusual when compared against a client’s expected pattern of activity.

Red Flags related to Due Diligence

- Clients who exhibit unusual concern in regard to compliance, with reporting requirements and the company’s anti-money laundering policies, particularly with respect to his/her identity, type of business and assets, reluctance or refusal to reveal any information concerning business activities;
- Information provided by the client that identifies a legitimate source for funds is false, misleading, or substantially incorrect;
- Clients who (or a person publicly associated with the client) have a questionable background or are the subject of news reports indicating possible criminal, civil, or regulatory violations;
- The client’s activity demonstrates outflows of funds or other assets well beyond the known income or resources of the client;
- Unsatisfactory or incomplete identification evidence;
- Reluctance or a refusal by a client to provide complete identification evidence; Clients asking staff to “bend” the rules;
- Unwillingness to disclose the source of funds;
- Unwillingness to disclose the identity of ultimate beneficial owners;
- Lack of adequate identification or source of funds being provided;
- Any action or request by a client which is inconsistent with your experience or knowledge of their business, affairs, income or previous history;
- The receipt or transmission of funds in circumstances which appear to have no commercial logic or perhaps involve jurisdictions which are renowned for money laundering.

Red Flags related to Excessive Secrecy

- Unnecessary granting of powers of attorney, in particular wide-ranging powers of attorney;
- Using different accounts to transfer the funds directly;
- A client tries to persuade an employee not to file required reports or maintain required records; A
- client is reluctant to provide information needed to file an internal report, in compliance with the requirements of legislation.

Red Flags related to Corporate Structures

- Subsidiaries which have no apparent purpose;
- Companies which continuously make substantial losses;
- Complex group structures without a cause;
- Uneconomic group structures for tax purposes;
- Frequent changes in shareholders and directors.

Red Flags related to Public Officials

- Clients who are public officials conducting business in the name of a family member who begins making large transfers not consistent with the known legitimate sources of income of the family;
- Clients who are related to public officials and make large transfers not consistent with his/her own legitimate sources of income.

6.6.3 Clients with heightened risk

Certain types of clients may inherently carry a heightened integrity risk, for example, operators of coffeeshops or sex clubs, commercial real estate activities. This is because the origins of the large amounts of incoming cash are harder to determine thus they carry a higher risk of fraud and money laundering. This means that the Company needs to take additional measures for these kinds of clients in order to mitigate the risk.

7. THE POLICY AND PROCEDURE FOR REPORTING SUSPICIOUS ACTIVITIES

7.1 Reporting Suspicious Activities- Internal Disclosure

Any information or other matter which gives rise to a knowledge or suspicion that a client is engaged in or attempting to engage in money laundering, terrorist financing or any other crime has to be reported to CO as soon as possible by completing the Internal Reporting Form ("Form") (Appendix 5).

Documenting one's suspicions ensures that the staff members and the Company are protected from criminal liability for failure to report. It is important that staff members do not delay documenting their concerns immediately. This can assist CO, and FIU, to act quickly and within the requirements of the applicable law.

After completing the Form, the staff member should sign and date it, obtain the signature of CO and receive a copy of the Form for their files. CO will acknowledge receipt of such reports and remind the staff member concerned not to do or say anything which might alert the client that he/she/it may be under investigation.

CO will then access the Form and he/she will decide whether a report should be made to FIU. Any internal disclosure report identified by CO as suspicious is directly submitted to FIU.

Further to that the Internal Suspicious report is thereafter duly filed and kept as per the Record Keeping Policy of the Company by the CO.

Amongst other things CO will consider:

- If any of the 'red flags' have been identified;
- Deviating behaviour on the part of the client, and activities that are illogical based on knowledge of the client or sector;
- The client makes use of legal persons or companies in which the control structure is not transparent or which, because of their nature or method of incorporation, are suitable for masking the identity of the underlying beneficial owner (e.g. bearer shares, trusts, foreign legal persons), without being able to give the Company an acceptable explanation for this;
- The frequent alteration of legal structures and/or changing of directors of legal persons or companies. There is a complex legal structure that does not appear to serve a genuine object; In addition to the indicators, the 'gut feeling' of employees and CO is also important

It is very important that Internal and External Reporting Forms are kept in files that are entirely separate from those of the client. It is the responsibility maintain and kept securely these files.

Failure to report suspicious activities or having a knowledge that the funds deposited in the Trading Account of Client are proceeds of felony or a misdemeanour and/or anyone who wilfully commits any of the following acts, shall be considered a perpetrator of the crime of money laundering.

A person is guilty of money laundering if, knowing or believing that property is or represents the benefit of criminal conduct or being reckless as to whether the property is or represents such benefit, the person, without lawful authority or excuse

- converts, transfers or handles the property, or removes it from the Republic;
- conceals or disguises the true nature, source, location, disposition, movement or ownership of the property or any rights with respect to it; or
- acquires, possesses or uses the property.

Removing property from the Republic shall include references to removing it from another country or territory and moving property within the Republic or a country or territory in preparation for or for the purpose of removing it from the Republic or the country or territory in question.

Any person who participates in such conduct as described above including but not limited to, aiding, abetting, assisting, attempting, counselling, conspiring, concealing or procuring the commission of such conduct commits the offence of money laundering as a principal offender and shall be liable to be tried and punished accordingly.

Further to that a failure to report suspicious activities is a serious failure that may cause imposition of penalties and or crime sentence based on the severity of the crime.

7.2 Reporting Suspicious Activities- External Disclosure

Anti-Money Landering Act 2020 ("Act 2020") creates an obligation on all Financial Institutions and other entities as identified by the Act 2020 as relevant entities, every reporting entity shall register with the

FIU. When submitting the report to the FIU the CO shall consider the following risks:

- The profile of its customers;
- The geographic area in which it conducts business;
- The products or product that it deals in;
- The means by which such products or services are delivered;
- The transaction that it conducts;
- Customer due diligence carried out by third parties, and;
- The technological developments in identifying such risks.
- The services or services that it provides or receives;

8. CLIENT DUE DILIGENCE AND IDENTIFICATION PROCEDURES

8.1 Cases for the application of Client Identification and Due Diligence Procedures

The Company shall duly apply Client identification procedures and Client due diligence measures in the following cases:

- when establishing a Business Relationship;
- when carrying out Occasional Transactions amounting to USD 10,000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
- when there is a suspicion of AML, regardless of the amount of the transaction;
- when there are doubts about the veracity or adequacy of previously Client identification data.

In this respect, it is the duty of the MLRO to apply all the relevant Client Due Diligence Identification Procedures of the Manual for the four (4) cases mentioned above. Furthermore, the MLRO shall also be responsible to collect and file the relevant Client identification documents, according to the recording keeping procedures in the Manual.

Further, the MLRO shall be responsible to maintain at all times and use during the application of Client Due Diligence and identification procedures template-checklists with respect to required documents and data from potential clients, as per the requirements of the applicable laws and regulations.

8.2 Ways of application of Client Identification and Due Diligence Procedures

Client identification procedures and client due diligence measures shall comprise:

Identifying the Client and verifying the client's identity on the basis of documents, data or information obtained from a reliable and independent source. It is noted that the identification procedure includes the following:

- Creation of an economic profile for the customer/beneficial owner;
- identifying the beneficial owner and taking risk-based and adequate measures to verify the identity on the basis of documents, data or information obtained from a reliable and

independent source so that the person carrying on in financial or other business knows who the beneficial owner is;

- as regards legal persons, trusts and similar legal arrangements, taking risk based and adequate measures to understand the ownership and control structure of the client;
- obtaining information on the purpose and intended nature of the business relationship;
- conducting on-going monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the information and data in the possession of the person engaged in financial or other business in relation to the client, the business and risk profile, including where necessary, the source of funds and ensuring that the documents, data or information held are kept up-to-date;
- Screening clients against databases or third party checks for adverse related news.

The Company applies each of the client due diligence measures and identification procedures set out above, but may determine the extent of such measures on a risk sensitive basis depending on the type of client, business relationship, product or transaction.

8.3 Identification and verification of the identity of applicants for business.

The Company identifies and verifies the identities of applicants for business whether they are Directors, Shareholders, Beneficial Owners, Settlers or Contributors of capital, Beneficiaries, Protectors, Enforcers, Trustees, Bank mandate and Power of Attorney holders, etc by verifying:

A. In case of natural persons:

- Full Name;
- Permanent residence address;
- Phone number
- Date of birth;
- Place of birth;
- Nationality;

Primary identity documentation for identity must be obtained and retained on these clients. They must be pre-signed, either in an original form or must be certified appropriately - and should bear a photograph of the principal. Primary identity documentations acceptable are:

- Current valid passports;
- National identity cards;
- Current valid driving licenses.

In addition to this primary identity documentation, the Company also obtains additional verification of identity information- secondary identity documentation. The secondary documentation must be, as for primary identity verification, either in an original form or must be appropriately certified. The following documentation is acceptable:

- A recent utility bill (which is less than 3 months old);
- A recent bank or credit card statement (as such P.O. Box addresses are not acceptable as permanent residential addresses of clients. Some countries have P.O. Box addresses such as in Middle East and Africa) (which is less than 3 months old);
- A recent bank statement (which is less than 3 months old);
- Alternative verification documentation acceptable is:
 - Obtaining a reference from a professional person who knows the principal. The reference must show the permanent residential address of the principal; Conducting a credit reference agency search;
 - Checking a current register of electors;
 - Utilizing an address verification service; or
 - Visiting the principal at the principal's permanent residential address.

B. In case if client is not an individual but is a legal person or arrangement:

i. Being a Private Company

- Obtain an original or appropriately certified copy of the certificate of incorporation or registration;
- Check with the relevant companies' registry that the company is validly existing;
- Obtain details of the registered office and place of business;
- Verify the identity of the principals of the company as (1) above;
- Verify that any person who purports to act on behalf of the company is so authorized, and identifying that person;

ii. Being a Trust

- Obtain an original or appropriately certified copy of a trust deed or pertinent extracts thereof;
- Where the trust is registered – check with the relevant registry to ensure that it does exist;
- Obtain details of the registered office and place of business of the trustee;
- Verify the identity of the principals of the trustee as per (1) and or (2) above.

iii. Being a Partnership

- Obtain an original or certified copy of the partnership deed;
- Obtain a copy of the latest report and accounts;
- Verification of the nature of the business of the partnership to ensure that it is legitimate;
- Verifying the identity of the significant partners (20% interest) as above;
- Verifying that any person that purports to act on behalf of the Partnership is



so authorized, and identifying that person.

8.4 Additional Due Diligence measures for financial institutions

The Company must undertake following additional due diligence measures while establishing and maintaining correspondent relationships:

- i. Obtaining sufficient information about a respondent institution to avoid any relationships with “shell-banks”;
- ii. Determining from publicly available sources of information the reputation of a respondent institution, including whether it has been subject to a money laundering or terrorist financing investigation or other regulatory action;
- iii. Assessing the respondent institution’s AML controls on a periodic basis;

The Company is bound to comply with the anti-money laundering regulations of FCA and international laws. As company is dealing with foreign financial brokerage firms we must monitor all financial transactions with utmost vigilance and must report suspicious activities to the concerned authorities.

8.5 Enhanced Customer Due Diligence (“EDD”)

EDD will be undertaken by the MLRO in the following situations:

- possible match on a Sanctions list. The profile for the potential match indicates negative information and the anti money laundering (“AML”)/know your customer (“KYC”) screening software hit cannot be definitively ruled out as a true match;
 - PEP match. The potential match is classified by the AML/KYC screening software as a PEP. An immediate family member of such person or a known close associate of such person also qualifies as a PEP.
 - questionable jurisdiction connection. The person is a citizen of a country of questionable reputé or without adequate anti-money laundering strategies, or resides there. The countries which qualify as “questionable” are determined by the MLRO from time to time, having regard to a number of resources, including the FATF recommendations;
 - questionable business activity. The person is involved in industries that are of questionable reputation, such as casinos or pornography, or is involved in a business that is highly cash intensive. Which business activities are questionable are determined by the compliance department from time to time, having regard to a number of resources, including the FATF's recommendations;
 - where jurisdictions have been identified by the FATF as jurisdictions that have not set up adequate systems to prevent money laundering and terrorist financing, this is seen as one of the factors increasing the risk of money laundering and terrorist financing in a business relationship;
- All High Risk clients will be recorded in the High Risk Clients Log (Appendix 1).

8.6 Politically Exposed Persons (PEPs)

A politically exposed person (PEP) is defined by the Financial Action Task Force (FATF) as an individual who is or has been entrusted with a prominent public function, as well as the immediate family members or

close associates of these individuals. Due to their position and influence, it is recognised that many PEPs are in positions that potentially can be abused for the purpose of committing money laundering offences and related predicate offences, including corruption and bribery, as well as conducting activity related to terrorist financing.

In light of the above when the Company enters into a business relationship with or provides services to PEPs additional identification measures must be taken as the business relationships entails a higher risk. The Company applies risk-based procedures and measures in order to be able to identify PEPs, and consequently determine the source of wealth and of funds that are used with the business relationship, and keep the business relationship under constant review.

A review is carried out both on acceptance and periodically to determine whether the client and the UBO qualify as PEPs. This applies equally to natural persons who may exert considerable influence on, hold considerable interests in and/or may strongly influence further reaching decisions of the unincorporated partnership, or who are able to control the partnership's policy to an essential degree. The depth of the due diligence varies depending on the risk profile of the client or UBO. In order to determine whether a particular client or UBO is a PEP, the Company amongst others steps performs number of screening lists internally prepared by the Financial institutions, lists issued by the local as well as international regulatory authorities such as notices from OFAC, UN and FSA as well as it uses World Check application.

All searches are then filed in the client's compliance file. The final decision to enter into a business relationship with PEP or to conduct a transaction for PEP must always be approved by the MLRO and the BoD. This also applies to a decision to continue a relationship with a customer who becomes PEP. Such approval is granted by the MLRO and the BoD. All PEPs will also be subject to ongoing monitoring.

All PEPs will be recorded in the PEPs Log (Appendix 2).

Any suspicious and/or unusual transaction to be reported to the Financial Investigation Unit ("FIU"). The Compliance Department is responsible to file Suspicious Transaction Report ("STR") with Central Bank using the online portal.

8.7 Third-Party Due Diligence and Identification Procedures

The Company shall obtain and verify sufficient information regarding third parties prior to entering into any contractual relationship.

Such information may include:

A. Legal and Corporate Documentation

- Certificate of Incorporation or equivalent registration document;
- Memorandum and Articles of Association or equivalent constitutional documents;
- Registered office address and principal place of business;

- Tax identification number, where applicable;
- Regulatory licenses and authorisations;
- Corporate structure chart, where appropriate.

B. Identification of Beneficial Owners and Management

The Company shall identify and verify:

- Directors;
- Ultimate Beneficial Owners (“UBOs”);

Verification shall be performed using reliable and independent documentation or electronic verification systems.

9. ON- GOING MONITORING

9.1 General

The Company has a full understanding of normal and reasonable account activity of its clients as well as of their economic profile and has the means of identifying transactions which fall outside the regular pattern of an account’s activity or to identify complex or unusual transactions or transactions without obvious economic purpose or clear legitimate reason. Without such knowledge, the Company shall not be able to discharge its legal obligation to identify and report suspicious transactions to the FIU.

The constant monitoring of the clients’ accounts and transactions is an imperative element in the effective controlling of the risk of AML.

In this respect, the MLCO shall be responsible for maintaining as well as developing the on-going monitoring process of the Company.

9.2 Procedures

The procedures and intensity of monitoring clients’ accounts and examining transactions on the client’s level of risk shall include the following:

- i. the identification of:
 - all high risk clients, as applicable;
 - the Company shall be able to produce detailed lists of high risk clients, so as to facilitate enhanced monitoring of accounts and transactions, as deemed necessary;
 - transactions which, as of their nature, may be associated with money laundering or terrorist financing;
 - unusual or suspicious transactions that are inconsistent with the economic profile of the client for the purposes of further investigation;
 - in case of any unusual or suspicious transactions, the person who identified the unusual or suspicious transactions shall be responsible to communicate

with the MLCO;

- ii. further to point (i) above, the investigation of unusual or suspicious transactions by the MLCO. The results of the investigations are recorded in a separate memo and kept in the file of the Clients concerned;
- iii. the ascertainment of the source and origin of the funds credited to accounts;
- iv. the on-going monitoring of the business relationship in order to determine whether there are reasonable grounds to suspect that client accounts contain proceeds derived from serious AML and/or tax offences;
- v. the use of appropriate and proportionate IT systems including:
 - adequate automated electronic management information systems which will be capable of supplying the BoD and the MLCO, on a timely basis, all the valid and necessary information for the identification, analysis and effective monitoring of client accounts and transactions based on the assessed risk for AML purposes, in view of the nature, scale and complexity of the Company's business and the nature and range of the investment services undertaken in the course of that business;
 - automated electronic management information systems to extract data and information that is missing regarding the Client identification and the construction of a Client's economic profile;
 - for all accounts, automated electronic management information systems to add up the movement of all related accounts on a consolidated basis and detect unusual or suspicious activities and types of transactions. This can be done by setting limits for a particular type, or category of accounts (e.g. high risk accounts) or transactions (e.g. deposits and withdrawals in cash, transactions that do not seem reasonable based on usual business or commercial terms, significant movement of the account incompatible with the size of the account balance), taking into account the economic profile of the client, the country of his origin, the source of the funds, the type of transaction or other risk factors. The Company shall pay particular attention to transactions exceeding the abovementioned limits, which may indicate that a client might be involved in unusual or suspicious activities.
- vi. the monitoring of accounts and transactions in relation to specific types of transactions and the economic profile, as well as by comparing periodically the actual movement of the account with the expected turnover as declared at the establishment of the business relationship. Furthermore, the monitoring covers clients who do not have a contact with the Company as well as dormant accounts exhibiting unexpected movements.

10. RECORD KEEPING

All records relating to internal decision-making, policy formulation, all documents obtained for the purpose of identification and all transaction data as well as other information related to money laundering matters, suspicious activity reports, records of AML/CTF training sessions shall be safeguarded in such a



way that only authorized employees have access to this information and documentation as well as in accordance with the applicable anti-money laundering laws/regulations.

All records will be stored either digitally or on paper, depending on the form in which information and documentation is available.

The records shall be stored in such a way that:

- i at the request of a supervisory institution, the data/information required is easily accessible and will provide sufficient evidence;
- ii any changes and modifications to the content can be easily identified;
- iii the information can not be manipulated or altered.

All records must be kept for period of not less than ten (10) years from the date of expiration/termination of the contractual relationship with the Client.

11. TRAINING

In view of the complexity of the business activities and the increased level of regulatory requirements that the Company is required to comply with, it is imperative that all the employees maintain a good level knowledge that enables them to effectively discharge their responsibilities. In particular, adequate knowledge and experience on the part of employees concerning the management of the risks of AML and ensuring a full compliance with the legal framework is something that the Company takes very seriously .

Thus the employees regularly attend educational courses which indispensable for their future development. The training programmes are focused not only on the legal and compliance framework within which the Company is required to operate but also on AML techniques, methods and trends, on the international context and standards, and on new developments.

Further, in order to assist employees in understanding of all policies and procedures, the Company provides anti money laundering and terrorism financing training sessions for employees. Attendance is required for all employees. The MLRO will keep records of all training sessions, including dates, times, locations and names of attendees.

All new staff will also receive an introduction to compliance and AML training by the Compliance Officer as soon as reasonably practical after joining the Company. This training will be arranged by the MLRO.

All relevant staff also received a regular refresher training to ensure that their knowledge is kept current with recent developments. The MLRO will organise and co-ordinate the necessary compliance training. The MLRO will also assess the need for further training.

Furthermore, all employees are expected to be fully aware of the Company's policies and procedures. Each employee is required to read and comply with the Manual, address any questions and concerns to the MLRO or and sign the acknowledgement form Appendix 3 confirming that he/she has read, understood and will comply with the Company's policies and procedures.

The Company maintains an ongoing Training Register, as set out in Appendix 4. Training records are kept



for the minimum period of ten (10) years.



APPENDIX 1- LOG OF HIGH-RISK CLIENTS

First Name	Middle Name	Surname	Client Number	Date Added	Reason for "high risk client status"



APPENDIX 2- PEP LOG

First Name	Middle Name	Surname	Client Number	Date Added	Reason for "PEP status"



APPENDIX 3- Acknowledgement Form

I, the undersigned, acknowledge that I have received, have read and have understood the Anti – Money Laundering Manual and Combating Terrorism Financing (the “Manual”). I will adhere to the policies and procedures set forth in the Manual. I have had an opportunity to clarify any questions, which I may have concerning the provisions of the Manual.

I further understand that the principles herein may be changed from time to time at the discretion of the MLRO with prior approval of the Board of Directors.

Employee name	Employee signature	Date
---------------	--------------------	------



APPENDIX 4 - Training Attendance Sheet

I, the undersigned, hereby confirm that I have attended the AML Staff Training which included inter alia information about prevention and suppression of AML, related legislation, offences, supervisory authorities, examples of AML, Company's updated AML Manual, due diligence procedures with respect to high-risk clients provided by Company's Anti-Money Laundering Compliance Officer.

No.	Date	Department	Full Name	Signature
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				



APPENDIX 5 – INTERNAL REPORTING FORM

Internal Reporting Form		
Your name and contact details:	Name	
	Department and position	
	Address	
	Tel No.	
	Email	
	Date	
The names of those involved (if known):		
Details of concerns:		
(Please provide full details of the suspicious activity: names, dates and places and the reasons why you consider this to be a suspicious activity together with any supporting evidence. Please <u>continue on</u> separate sheet if necessary.		

Full Name of the Employee	
Signature	
Date and Place	

Full Name of the Compliance Officer	
Signature	
Date and Place	